UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
MIAMI DIVISION

In re Lakeview Loan Servicing Data Breach Litigation	**CASE NO. 1:22-CV-20955-DPG** **CONSOLIDATED CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Evelyn Rivera, Stephanie Stone, Jorge Gonzalez, Robert Keach, Cindy Villanueva, Deborah Hamilton, Michael Kassem, Beth Berg, Savannah Farley, Kristine Milewski, Thomas Lapenter, Emily Holt, Hardik Sevak, William Blando, Julie Abraham, Peter Wojciechowski, Kimberley Rowton, Dylan Normile, Jessica Valente-Brodrick, April Burnett, Denise Scott, Julia Franke, Ashley Cashon, Richard Cashon, Nilsa Misencik, Robert Martin, Christopher Sparks, David Kraus, John McMahon, Shannon Thomas, Mathew Myers, Jay Saporta, and Derek Crenshaw ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Consolidated Class Action Complaint against Lakeview Loan Servicing, LLC ("Lakeview"), Pingora Loan Servicing, LLC ("Pingora"), and Bayview Asset Management LLC ("Bayview" and, collectively with Lakeview and Pingora, "Defendants") and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This action stems from Defendants' failure to secure the sensitive personal information of their current and former customers and other consumers for whom Defendants performed services. Defendants Lakeview and Pingora are mortgage loan servicers and Lakeview

is the fourth largest mortgage loan servicer in the United States.[1]

2. Lakeview and Pingora are both subsidiaries of Bayview. Lakeview and Pingora obtain certain personally identifying information related to their customers—current and former mortgagees, as well as mortgage applicants—in furtherance of services they perform on their behalf.

3. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard sensitive personally identifiable information provided by and belonging to their customers, including, without limitation, name, address, loan number, and Social Security number and, for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing (collectively, "PII").

4. On or around October 27, 2021, an intruder gained entry to Defendants' network systems, accessed the PII stored therein, and exfiltrated information (the "Data Breach"). In early December 2021, Defendants identified this "security incident involving unauthorized access to [their] file servers."[2] Defendants determined that "an unauthorized person obtained access to files on [their] file storage servers from October 27, 2021 to December 7, 2021."[3]

5. On January 31, 2022, the review process generated a preliminary list of individuals affected by the Data Breach. Defendants determined that the unauthorized actor accessed and exfiltrated the PII of at least 2,537,261 current and former Lakeview customers, including that of Plaintiffs Evelyn Rivera, Stephanie Stone, Jorge Gonzalez, Robert Keach, Cindy Villanueva, Deborah Hamilton, Michael Kassem, Beth Berg, Savannah Farley, Kristine Milewski, Thomas Lapenter, Emily Holt, Hardik Sevak, William Blando, Julie Abraham, Peter Wojciechowski,

[1] *See* https://lakeview.com (last visited July 7, 2022).
[2] Exhibit ("Ex.") 1 (sample "Notification Letters" sent to California Attorney General's Office).
[3] *Id*.

Kimberley Rowton, Dylan Normile, Jessica Valente-Brodrick, April Burnett, Denise Scott, Julia Franke, Richard Cashon, Ashley Cashon, Nilsa Misencik, Robert Martin, Christopher Sparks, David Kraus, John McMahon, Shannon Thomas, Mathew Myers, Jay Saporta, and Derek Crenshaw, which Lakeview reported to various state Attorneys General on March 18, 2022. Months later, on June 23, 2022, Lakeview reported that an additional 100,796 Lakeview customers were impacted. Defendants also determined that 1,268,248 Pingora customers were affected, including numerous Plaintiffs and consumers nationwide.[4] The current and former customers of Lakeview and/or Pingora are referenced below as the "Class Members."

6. On or around March 16, 2022, Lakeview began notifying Plaintiffs and Class Members of the Data Breach. On or around April 6, 2022, Pingora began notifying Plaintiffs and Class Members of the Data Breach. Lakeview issued additional notices beginning in June 2022.

7. In the notices sent to Plaintiffs and Class Members, Lakeview and Pingora recognized that each Class Member is now subject to the present and continuing risk of identity theft and fraud, by offering Plaintiffs and Class Members limited identity theft protection from Kroll, who Defendants consider a "fraud specialist." Lakeview and Pingora also directed Plaintiffs and Class Members "to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity." The offered services, however, fall well short of what is needed to protect Plaintiffs and Class Members from the lifelong implications of having their most private PII accessed, acquired, exfiltrated, and/or published on the internet. As one element of damages, Plaintiffs and Class Members seek a sum of money sufficient to provide to Plaintiffs and Class Members enhanced identity theft protection services

[4] OFFICE OF THE INDIANA ATTORNEY GENERAL, Security Breaches *available at* https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/JulyYear-to-date-Report.pdf. (last visited July 22, 2022).

for their respective lifetimes.

8. Bayview's Security Operations Center (the "Bayview SOC") "protect[s] the Bayview brand and assets."[5] The Bayview SOC's responsibilities include the following:

a. "[E]nsure the monitoring and analysis of incidents to protect People, Technologies and Process addressing all security incidents and ensuring timely escalation."

b. "Direct the Cyber Intelligence capability to identify potential threats delivering strategic reports and strategies to minimize the impact of the threat."

c. "Leveraging experience in incident response, forensics, security analysis, and security engineering to support the IR department in developing people, processes, and technology to protect the Bayview brand and assets."

d. "Ensuring daily management, administration & maintenance of security devices to achieve operational effectiveness."

e. "Ensuring threat management, threat modeling, identify threat vectors and develop use cases for security monitoring."

9. Analysts within the Bayview SOC "investigate cybersecurity and/or computer network-related incidents" and "perform daily incident response triage communicating accordingly as needed."[6] Their duties include the following:

a. "Conduct proactive monitoring, investigation, and mitigation of security incidents."

b. "Recognize potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses or relevant event detail and

[5] *See* https://careers.bayview.com/bam/jobs/4592?lang=en-us (last visited July 29, 2022).
[6] *See* https://careers.bayview.com/bam/jobs/4593?lang=en-us (last visited July 29, 2022).

summary information."

c. "Enhance security operations, analytics, threat hunting, and security orchestration and automation capabilities."

10. Lakeview, like Bayview, invites applicants to apply for positions in the Bayview SOC, indicating that Lakeview, like Bayview, relies on the Bayview SOC to identify potential security threats and respond to security incidents.[7]

11. Bayview also has a "research team" that relies on engineers to "develop, maintain, and enhance the various databases used to monitor the performance of consumer loans, to improve data pipelines for efficient uploading and downloading of data, to clean the data for use by the research and trading teams, and to help automate reporting data and visualization."[8] These analysts also "[i]ntegrate data from multiple sources to meet business requirements."

12. Lakeview, like Bayview, invites applicants to apply for positions on the Bayview research team, indicating that Lakeview, like Bayview, relies on the Bayview research team for data integration and management.[9]

13. Regardless of whether it was initially collected and/or maintained by Bayview, Lakeview, and/or Pingora, Plaintiffs' and Class Members' PII was among the "Bayview brand and assets" that the Bayview SOC was supposed to, but failed to, protect.

14. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties to these individuals to safeguard

---

[7] *See* https://lakeview-loan-servicing.talentify.io/job/security-operations-center-manager-coral-gables-florida-lakeview-loan-servicing-4592?currentPage=2 (last visited July 29, 2022); https://lakeview-loan-servicing.talentify.io/job/security-operations-center-analyst-coral-gables-florida-lakeview-loan-servicing-4593?currentPage=3 (last visited July 29, 2022).

[8] *See* https://careers.bayview.com/bam/jobs/4505?lang=en-us (last visited July 29, 2022).

[9] *See* https://lakeview-loan-servicing.talentify.io/job/data-engineer-coral-gables-florida-lakeview-loan-servicing-4505?currentPage=3

and protect the PII from unauthorized access. Defendants admit that the unencrypted PII accessed and exfiltrated includes highly sensitive information, such as names, dates of birth, addresses, phone numbers, financial or bank account information, Social Security numbers, insurance information and account numbers, medical information including medical history, condition, treatment and diagnosis, medical record numbers, driver's license numbers, and email addresses.

15. The exposed PII of Plaintiffs and Class members can be and in certain cases has been sold to other identity thieves or on the dark web, a hidden network of black-market websites that serves as a "haven for all kinds of illicit activity (including the trafficking of stolen personal information captured through means such as data breaches or hacks)."[10]

16. Plaintiffs John McMahon and Jay Saporta are informed and believe that their information has already been placed onto the dark web. Hackers can now access and/or offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class members face an ongoing and lifetime risk of identity theft, which is heightened by the loss of their Social Security numbers.

17. This PII was compromised due to Defendants' negligent and/or careless acts and omissions and their failure to protect PII of Plaintiffs and Class Members .

18. Until notified of the breach, Plaintiffs and Class Members had no idea that their PII had been compromised by the Data Breach and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. This risk will remain for their rest of their lives.

19. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiffs' and Class members;

[10] https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited July 22, 2022).

(ii) warn Plaintiffs and Class members of their inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities. Defendants' conduct amounts to at least negligence and violates federal and state statutes designed to prevent or mitigate this very harm.

20. Plaintiffs and Class Members have suffered actual and present injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft for their respective lifetimes; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the present and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of their personal data entrusted to Defendants on the mutual understanding that Defendants would safeguard their PII against theft and not allow access to and misuse of their personal data by others; and (h) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further injurious breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII. Plaintiffs and Class Members, at the very least, are entitled to damages and injunctive relief tailored to address the vulnerabilities exploited in the breach, and designed to protect Plaintiffs' and Class Members' PII, as well as an order from the Court directing the destruction and deletion of all PII for which Defendants cannot demonstrate a reasonable and legitimate purpose for continuing to maintain possession of such PII.

21. Defendants understand the need to protect the privacy of their customers and use

security measures to protect their customers' information from unauthorized disclosure.[11] And as sophisticated financial entities who maintain private and sensitive consumer information, Defendants further understood the importance of safeguarding PII. Yet Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through access to and exfiltration by an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

22. Plaintiffs by this action seek compensatory damages together with injunctive relief to remediate Defendants' failures to secure their and the other Class Members' PII, and to provide damages, for among other things, for Plaintiffs and Class Members to secure identity theft insurance, and credit repair services for Class Members' respective lifetimes to protect the Class of Data Breach victims from identity theft and fraud.

II. PARTIES

Plaintiff Evelyn Rivera

23. Plaintiff Evelyn Rivera is a resident and citizen of the State of Massachusetts.

24. Plaintiff Rivera received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan

[11] *See* Ex. 2 ("Privacy Policy").

number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Stephanie Stone

25. Plaintiff Stephanie Stone is a resident and citizen of the State of Texas.

26. Plaintiff Stone received a letter dated March 21, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Jorge Gonzalez

27. Plaintiff Jorge Gonzalez is a resident and citizen of the State of Texas.

28. Plaintiff Gonzalez received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Robert Keach

29. Plaintiff Robert Keach is a resident and citizen of the State of California.

30. Plaintiff Robert Keach received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Cindy Villanueva

31. Plaintiff Cindy Villanueva is a resident and citizen of the State of California.

32. Plaintiff Villanueva received a letter from Defendant Lakeview dated March 17, 2022 concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Deborah Hamilton

33. Plaintiff Deborah Hamilton is a resident and citizen of the State of Georgia.

34. Plaintiff Hamilton received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Michael Kassem

35. Plaintiff Michael Kassem is a resident and citizen of the State of Georgia.

36. Plaintiff Kassem received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Beth Berg

37. Plaintiff Beth Berg is a resident and citizen of Illinois.

38. Plaintiff Berg received a letter dated March 21, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained names, addresses, loan numbers, Social Security numbers, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Savannah Farley

39. Plaintiff Farley is a resident and citizen of Indiana.

40. Plaintiff Farley received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview network. The compromised files contained names, addresses, loan numbers, Social Security numbers, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Kristine Milewski

41. Plaintiff Kristine Milewski is a resident and citizen of the State of Delaware.

42. Plaintiff Milewski received a letter dated April 4, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Thomas Lapenter

43. Plaintiff Thomas Lapenter is a resident and citizen of the State of New Jersey.

44. Plaintiff Lapenter received a Data Breach notification letter dated April 6, 2022 from Defendant Pingora. The letter stated that unauthorized actors gained access to files on Pingora's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Emily Holt

45. Plaintiff Emily Holt is a resident and citizen of the State of New Jersey.

46. Plaintiff Holt received a letter dated June 10, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Hardik Sevak

47. Plaintiff Hardik Sevak is a resident and citizen the State of New York.

48. Plaintiff Sevak received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, and Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff William Blando

49. Plaintiff William Blando is a resident and citizen of the State of Missouri.

50. Plaintiff Blando received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Julie Abraham

51. Plaintiff Julie Abraham is a resident and citizen of the State of Michigan.

52. Plaintiff received a letter from Defendant Pingora dated April 6, 2022 concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Peter Wojciechowski

53. Plaintiff Peter Wojciechowski is a resident and citizen of the State of Florida.

54. Plaintiff Wojciechowski received a letter from Defendant Lakeview dated March 18, 2022 concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Kimberley Rowton

55. Plaintiff Kimberley Rowton is a resident and citizen of the State of Virginia.

56. Plaintiff Rowton received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Dylan Normile

57. Plaintiff Dylan Normile is a resident and citizen of the State of Virginia.

58. Plaintiff Normile received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Jessica Valente-Brodrick

59. Plaintiff Jessica Valente-Brodrick is a resident and citizen of the State of Arizona.

60. Plaintiff Jessica Valente-Brodrick's husband received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach, but Defendant did not send her a separate, additional letter. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff April Burnett

61. Plaintiff April Burnett is a resident and citizen of the State of Tennessee.

62. Plaintiff Burnett received a letter dated April 4, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Denise Scott

63. Plaintiff Denise Scott is a resident and citizen of the State of Florida.

64. Plaintiff Scott received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Julia Franke

65. Plaintiff Julia Franke is a resident and citizen of Florida.

66. Plaintiff Franke received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network. The compromised files contained names, addresses, loan numbers, Social Security numbers, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiffs Ashley and Richard Cashon

67. Plaintiffs Ashley and Richard Cashon are residents and citizens of the State of South Carolina.

68. Plaintiffs received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Nilsa Misencik

69. Plaintiff Nilsa Misencik is a resident and citizen of the State of South Carolina.

70. Plaintiff Misencik received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Robert Martin

71. Plaintiff Robert Martin is a resident and citizen of the State of South Carolina.

72. Plaintiff Martin received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Christopher Sparks

73. Plaintiff Christopher Sparks is a resident and citizen of the State of Alabama.

74. Plaintiff Sparks received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff David Kraus

75. Plaintiff David Kraus is a resident and citizen of the State of Pennsylvania.

76. Plaintiff Kraus received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff John McMahon

77. Plaintiff John McMahon is a resident and citizen of Maryland.

78. Plaintiff McMahon received a letter dated March 16, 2022 from Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained names, addresses, loan numbers, Social Security numbers, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Shannon Thomas

79. Plaintiff Shannon Thomas is a resident and citizen of the State of Ohio.

80. On or around March 18, 2022, Plaintiff Thomas received a letter from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained names, addresses, loan numbers, Social Security numbers, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Mathew Myers

81. Plaintiff Mathew Myers is a resident and citizen of the State of Texas.

82. Plaintiff Myers received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Jay Saporta

83. Plaintiff Jay Saporta is a resident and citizen of the State of California.

84. Plaintiff Saporta received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Derek Crenshaw

85. Plaintiff Derek Crenshaw is a resident and citizen of the State of California.

86. Plaintiff Crenshaw received a letter dated March 17, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview Loan Servicing's network. The compromised files contained name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Defendant Lakeview Loan Servicing, LLC

87. Defendant Lakeview Loan Servicing, LLC is a private mortgage loan servicer organized under the laws of Florida, headquartered at 4425 Ponce de Leon Blvd, Coral Gables, FL 33146, with its principal place of business in Coral Gables, Florida.

88. Lakeview is a Delaware limited liability company and is wholly-owned by Bayview MSR Opportunity Corp., which is a Delaware corporation with its principal place of business in Coral Gables, Florida.

89. All of Plaintiffs' claims stated against Defendant Lakeview herein are also asserted against any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

Defendant Pingora Loan Servicing, LLC

90. Defendant Pingora Loan Servicing, LLC is a private mortgage loan servicer organized under the laws of Delaware, headquartered at 1819 Wazee Street, 2nd Floor, Denver, CO 80202, with its principal place of business in Denver, Colorado.

91. Pingora is wholly owned by Bayview Asset Management, LLC.

92. All of Plaintiffs' claims stated against Defendant Pingora herein are also asserted against any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

Defendant Bayview Asset Management, LLC

93. Defendant Bayview Asset Management, LLC is an investment management services company organized under the laws of Florida, headquartered at 4425 Ponce de Leon Blvd, Coral Gables, FL 33146.

94. Bayview is the parent company of Lakeview and Pingora, and as such controls Lakeview and Pingora and has responsibility for network security and the security of consumer information maintained by or on behalf of Lakeview and Pingora

95. All of Plaintiffs' claims stated against Defendant Bayview herein are also asserted against and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

96. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 Class Members and because the amount in controversy exceeds $5,000,000.00 exclusive of interest and costs. Moreover, the minimal diversity requirement is met as Plaintiffs, Class Members, and Defendants are citizens of different states.

97. The Court has personal jurisdiction over Defendants Lakeview and Bayview because, personally or through their agents, Defendants Lakeview and Bayview operated, conducted, engaged in, or carried on a business or business venture in Florida; had offices in Florida; committed tortious acts in Florida; and/or breached a contract in Florida by failing to perform acts required by the contract to be performed in Florida. Defendants Lakeview and Bayview are also headquartered in Coral Gables, FL.

98. The Court has personal jurisdiction over Defendant Pingora because, personally or through its relationship to and the control over it exercised by Bayview, Defendant Pingora

operated, conducted, engaged in, or carried on a business or business venture in Florida; committed tortious acts in Florida; and/or breached a contract in Florida by failing to perform acts required by the contract to be performed in Florida.

99. Venue is proper in this district under 28 U.S.C. § § 1391(a)(1), 1391(b)(1), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this district, and Defendants Lakeview and Bayview conduct substantial business in this district and reside in this district. Further, on information and belief, decisions regarding the management of the information security of Plaintiffs' and Class Members' PII were made by Bayview within this district. Moreover, it is believed that Defendants maintain Plaintiffs' and Class Members PII in the district, and the harm caused to Plaintiffs and Class Members emanated from this district.

IV. FACTUAL ALLEGATIONS

Background

100. Defendant Lakeview is the fourth largest mortgage loan servicer in the United States.[12] Lakeview owns the servicing rights to millions of Americans' mortgage loans. It partners with "several Servicing partners to process payments, manage the escrow, and provide customer service for [more than 1.4 million individuals'] existing mortgage[s]" per year.[13]

101. Bayview—Lakeview's parent company—acquired Pingora Holdings, L.P. and its wholly-owned subsidiary, Defendant Pingora Loan Servicing, LLC, from Annaly Capital Management, Inc. in July 2017 to expand its presence in the mortgage loan industry.

102. Plaintiffs and Class Members who received or applied for mortgage related services

[12] *See* https://lakeview.com (last visited July 26, 2022).
[13] *Id.*

from Lakeview or Pingora, or their mortgage loans or the servicing rights and responsibilities for those loans were acquired by Lakeview or Pingora. Thus, Plaintiffs were required to entrust some of their most sensitive and confidential information to the care of Defendants, including, without limitation: name, address, loan number, Social Security number, and additional information provided in connection with a loan application, loan modification, or other items necessary for loan servicing. Much of the information Plaintiffs and Class Members entrusted to Lakeview and Pingora is static, does not change, and can be used to commit myriad financial crimes.

103. In providing services to Plaintiffs and Class Members, Lakeview and Pingora generated and retained additional sensitive personal information about Plaintiffs and Class Members, including information concerning their loan services and information provided to them by their affiliates and sub servicers.

104. Sophisticated companies like Defendants are aware of the different types of threat actors acting across the Internet and the type of criminal cybersecurity acts they employ for profit. Accordingly, it is imperative that Defendants guard against those criminal exploits.

105. Plaintiffs and Class Members, as current and former customers of Defendants or their affiliates, relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

106. Defendants had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties. Defendants collected, maintained, and profited from information that they knew to be private and sensitive, and they were aware of the consequences to Plaintiffs and Class Members if they failed to adequately protect that information. Defendants breached their duty to Plaintiffs and Class Members and allowed an attacker access to

its systems for months without detection.

107. Defendants knew that the PII they maintained was a target of data thieves and that they had a duty to protect Plaintiffs' and Class Members' PII from unauthorized access. For example, Defendant Lakeview posts a Privacy Policy on its website.[14] The Privacy Policy promises consumers that Lakeview, "protect[s] your personal information from unauthorized access and use, [and] use[s] security measures that comply with federal law. These measures include computer safeguards and secured files and buildings." The Privacy Policy also acknowledges that Lakeview collects consumer data directly from consumers and via its affiliates. Specifically, Lakeview acknowledges that it collects information when consumers pay bills or apply for a loan, provide income or employment information.[15]

108. The Privacy Policy also provides a list of instances in which disclosure of PII could be made to its affiliates and other entities without prior written authorization—none of which is applicable here.[16]

109. Moreover, Defendants are sophisticated companies that knew or should have known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

110. There were a record 1,862 data breaches last year (2021), surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.

111. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January

[14] *See* Ex. 2.
[15] *Id.*
[16] *Id.*

2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

112. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service regularly issue warnings to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

113. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

The Data Breach

114. On or around October 27, 2021, an intruder gained unauthorized access to Defendants' network.[17] Defendants discovered the intrusion on or around December 7, 2021.[18] Before that discovery, the intruder accessed and exfiltrated the PII of at least 2,638,057 current and former Lakeview customers and 1,268,248 current and former Pingora customers.[19][20]

[17] Ex. 3 (sample "Notice of Data Breach" sent to Maine Attorney General's Office); *see also* https://oag.ca.gov/ecrime/databreach/reports/sb24-552339 (Pingora); https://oag.ca.gov/ecrime/databreach/reports/sb24-551822 (Lakeview) (last visited July 21, 2022).

[18] *Id.*

[19] OFFICE OF THE MAINE ATTORNEY GENERAL, Data Breach Notification, *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/3d0c184e-e78c-4123-8ce8-8535f71facd3.shtml; (initially reporting 2,537,261 impacted individuals); https://apps.web.maine.gov/online/aeviewer/ME/40/4e99b62d-cbb6-425c-a79d-3ad83b8533b1.shtml (adding an additional 100,796 impacted individuals) (last visited July 21, 2022).

[20] OFFICE OF THE INDIANA ATTORNEY GENERAL, Security Breaches *available at* https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/JulyYear-to-date-Report.pdf. (last visited July 21, 2022).

115. On or around March 18, 2022, Lakeview reported the Data Breach to the attorneys general offices of California,[21] Maine,[22] Massachusetts,[23] and Vermont, among other states.[24] On or about that date, it also began notifying Plaintiffs and Class Members of the Data Breach.

116. Beginning on or around March 16, 2022 and again on June 23, 2022 following Lakeview's discovery of an additional 100,796 victims, Lakeview sent Plaintiffs and Class Members a form "Notice of Data Breach" substantially similar to the sample letters provided to the state Attorneys General.[25]

117. The sample letters slightly varied in length and detail provided. The sample letter to the California Attorney General's Office stated in part:

> Lakeview Loan Servicing, LLC ("Lakeview") understands the importance of protecting the information we maintain. We are writing to inform you of an incident that involved some of your information. This notice explains the incident, measures we have taken, and steps that you may consider taking.
>
> **What Happened?**
>
> Lakeview owns the servicing rights to your mortgage loan. A security incident involving unauthorized access to our file servers was identified in early December 2021. Steps were immediately taken to contain the incident, notify law enforcement, and a forensic investigation firm was engaged. The investigation determined that an unauthorized person obtained access to files on our file storage servers from October 27, 2021 to December 7, 2021. The accessed files were then reviewed by our investigation team to identify the content.
>
> **What Information Was Involved?**
>
> On January 31, 2022, the review process generated a preliminary list of individuals, including you, whose name, address, loan number, and Social Security number were included in the files. We then took

[21] Ex. 1.
[22] Ex. 3.
[23] Ex. 4 (sample "Notice of Data Breach" sent to Massachusetts Attorney General's Office).
[24] Ex. 5 (sample "Notice of Data Breach" sent to Vermont Attorney General's Office).
[25] *See* Ex. 4.

> extensive measures to review that list to ensure accuracy and prepare the list to be used to mail notification letters. For some, the accessed files may also have included information provided in connection with a loan application, loan modification, or other items regarding loan servicing. The additional loan related information in the files is not the same for all individuals.
>
> **What We Are Doing.**
>
> We regret that this incident occurred and apologize for any inconvenience. Additional steps are being taken to further enhance our existing security measures.[26]

118. Lakeview admitted in the sample letter that unauthorized third persons accessed and removed from its network systems sensitive information about current and former customers of Lakeview and its affiliates, including, without limitation: "name, address, loan number, and Social Security number" and, for some, "information provided in connection with a loan application, loan modification, or other items regarding loan servicing."[27] Much of this sensitive information is static, cannot change, and can be used to commit myriad financial crimes.

119. Pingora began notifying its customers and those of its affiliates of the Data Breach on April 6, 2022 through letters substantially similar to the Lakeview notification letters.[28]

120. Plaintiffs' and Class Members' unencrypted information has already been leaked onto the dark web (as evidenced by the dark web notifications received by multiple Plaintiffs described below), and/or may simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of the affected current and former customers. Unauthorized individuals can access the PII of Plaintiffs and Class Members now that it has been stolen.

---

[26] *Id.* at 1.
[27] *Id.*
[28] *See* OFFICE OF THE NEW HAMPSHIRE ATTORNEY GENERAL, Data Breach Notification, *available at* https://www.doj.nh.gov/consumer/security-breaches/documents/pingora-loan-servicing-20220406.pdf (last visited July 7, 2022).

121. Defendants did not use reasonable security procedures and practices suitable or adequate to protect the sensitive, unencrypted information it was maintaining for consumers, causing the access and/or exfiltration of the PII of more than 2,638,057 individuals with Lakeview accounts and 1,268,248 individuals with Pingora accounts.

Defendants Acquire, Collect and Store Plaintiffs' and Class Members' PII.

122. Defendants acquired, collected, and stored the PII of Lakeview's and Pingora's current and former customers and those of its affiliates.

123. As a condition of receiving services from Lakeview and Pingora, Defendants (by way of their affiliate mortgage lenders) require that consumers entrust them with highly confidential PII.

124. By obtaining, collecting, and storing Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

125. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

126. Defendants could have prevented this Data Breach by properly securing and encrypting Plaintiffs' and Class Members' PII. Additionally, Defendants could have destroyed data, including old data that Defendants had no legal right or responsibility to retain.

127. Defendants' negligence in safeguarding Plaintiffs' and Class Members' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data,

especially sensitive financial data.

128. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

129. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[29] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, [and] employer or taxpayer identification number."[30]

130. The ramifications of Defendants' failure to keep secure Plaintiffs' and Class Members' PII are long lasting and severe. Once Social Security numbers and other PII have been stolen, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

131. PII is very valuable to criminals, as evidenced by the prices they will pay for it on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information is sold at prices ranging from $40 to $200, and bank details have a price range of $50 to $200.[31] Experian reports that a stolen credit or debit card number can sell for $5

[29] 17 C.F.R. § 248.201 (2013).
[30] *Id.*
[31] *Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 7, 2022).

to $110 on the dark web.[32] Criminals also can purchase access to entire sets of information obtained from company data breaches from $900 to $4,500.[33]

132. Social Security numbers are among the most sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[34]

133. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against potential misuse of a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.

134. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited

---

[32] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 7, 2022).
[33] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 7, 2022).
[34] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed July 7, 2022).

into the new Social Security number."[35]

135. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, in that situation, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, birthdate, financial history, and Social Security number.

136. This data commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[36]

137. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

138. The PII of Plaintiffs and Class Members was taken by hackers to engage in identity theft and/or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

139. Further, there may be a time lag between when harm occurs and when it is discovered and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit

[35] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed July 7, 2022).

[36] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed July 7, 2022).

> identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[37]

140. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Lakeview's and Pingora's current and former customers' PII, including Social Security numbers and financial account information, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Lakeview's and Pingora's current and former customers as a result of such a breach.

141. Plaintiffs and Class Members now face a lifetime of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damage in addition to any fraudulent use of their PII.

142. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on their network, comprising millions of individuals' detailed and confidential personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

143. Although Defendants have offered identity monitoring services for a limited time through Kroll, the offered services are inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the highly sensitive nature of the PII at issue here.

144. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of

---

[37] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last visited July 7, 2022).

Lakeview's and Pingora's current and former customers.

V. PLAINTIFF-SPECIFIC ALLEGATIONS

Plaintiff Evelyn Rivera's Experience

145. Plaintiff Rivera used Lakeview's services when she took out a mortgage on her home. As a condition to receiving loan services from Lakeview, Plaintiff Rivera provided her PII to Lakeview which was then entered into Lakeview's database and maintained by Lakeview.

146. Plaintiff Rivera greatly values her privacy and PII, especially when receiving loan and other financial services. Prior to the Data Breach, Plaintiff Rivera took reasonable steps to maintain the confidentiality of her PII.

147. Plaintiff Rivera received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

148. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Rivera faces, Defendant offered her a two-year subscription to a credit monitoring service.

149. In February 2022, Plaintiff Rivera experienced identity fraud in the form of an unauthorized $200 charge on her debit card for her checking account. As a result, she was required to obtain a new debit card. She believes the unauthorized $200 charge on her debit card is a result of the Data Breach given that it occurred relatively soon after the Data Breach, and she had no other previous fraudulent charges on her debit card.

150. About a week later, Plaintiff Rivera noticed another $200 charge on her account. She initiated the process of getting a new debit card a second time.

151. Over the course of the first few months of 2022, Plaintiff Rivera had to change her debit card for her bank account three times as she continued to notice $200 charges on her account approximately three times. She spent time in connection with the debit card replacements and her other actions in response to the Data Breach.

152. Since learning of the Data Breach, Plaintiff Rivera has spent additional time reviewing her bank statements and credit cards. Since February 2022, she has spent approximately two hours every day reviewing her bank, credit and debit card statements; procuring a new debit card from her bank—three times; and going to her bank to initiate investigations into the unauthorized charges. Plaintiff spent this time at Lakeview's direction In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

153. Plaintiff Rivera also noticed a $360 withdrawal from her CashApp account in February 2022. She had to cancel that account and its associated card and create a new account and request a new card from CashApp. The CashApp account was originally linked to her Lakeview account. An investigation concluded that the charge was fraudulent and not actually incurred by her.

154. Plaintiff Rivera has experienced an increase of other spam calls, text messages and emails after the Data Breach.

155. Plaintiff Rivera has received numerous emails showing transactions and invoices using her name and email, for which she is not responsible.

156. The Data Breach has caused Plaintiff Rivera to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

157. Plaintiff Rivera plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

158. Additionally, Plaintiff Rivera is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

159. Plaintiff Rivera stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

160. Plaintiff Rivera has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Stephanie Stone's Experience

161. Defendant Lakeview is the servicer of Plaintiff Stone's mortgage loan. As a condition to providing Plaintiff Stone loan services, Plaintiff Stone provided Lakeview with her PII, which it then entered into its database and maintained.

162. Plaintiff Stone provided Defendant Lakeview with significant personal, income, and financial information.

163. Plaintiff Stone greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Stone took reasonable steps to maintain the confidentiality of her PII.

164. Plaintiff Stone received a Notification Letter on or around April 4, 2022, dated March 21, 2022, from Defendant Lakeview concerning the Data Breach. The Notification Letter stated that unauthorized actors gained access to files on Lakeview's network that contained her

name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

165. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Stone faces, Defendant offered her a one-year membership to credit monitoring services. The offer is inadequate because data breach victims commonly face multiple years of ongoing identity theft.

166. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach.

167. In November 2021, bad actors began accessing multiple accounts owned by Plaintiff Stone, and they continue to do so. The bad actors attempted to open fraudulent accounts using Plaintiff Stone's PII. Plaintiff Stone had to file multiple police reports because of the bad actors' fraudulent actions.

168. As a result of the Data Breach, Plaintiff Stone must monitor her accounts and credit scores and has sustained emotional distress. It was also necessary for Plaintiff Stone to place credit holds with the three credit reporting agencies. Plaintiff Stone will need to spend additional time and effort opening new accounts. Plaintiff Stone intends to additional spend time taking steps to protect her PII in the future. Because of the Data Breach, Plaintiff Stone spent valuable time she otherwise would have spent on other obligations.

169. Moreover, Plaintiff Stone spent this time at Lakeview's direction. In the notice letter Plaintiff Stone received, Lakeview directed Plaintiff Stone to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

170. Plaintiff Stone also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant in order to

obtain services from Defendant, which was compromised in and as a result of the Data Breach.

171. Plaintiff Stone suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

172. Plaintiff Stone has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number in the hands of criminals.

173. Because of the Data Breach, Plaintiff Stone is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

174. Additionally, Plaintiff Stone typically takes measures to protect her PII and is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

175. Plaintiff Stone stores any documents containing her PII in a safe and secure location. She diligently chooses unique usernames and passwords for her online accounts. Further, Plaintiff Stone's field of expertise is information technology and she is well aware of the measures that companies like Defendant need to take in order to avoid disclosure of their clients' PII to dangerous cyber actors.

176. Plaintiff Stone has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Jorge Gonzalez's Experience

177. Plaintiff Gonzalez used Lakeview's services when his home mortgage was transferred to Lakeview. As a condition to receiving loan services from Lakeview, Plaintiff Gonzalez provided his PII to Lakeview, which was then entered into Lakeview's database and

maintained by Lakeview.

178. Plaintiff Gonzalez greatly values his privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Gonzalez took reasonable steps to maintain the confidentiality of his PII.

179. Plaintiff Gonzalez received a letter dated March 18, 2022, from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

180. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Gonzalez faces, Defendant offered him a one-year subscription to a credit monitoring service. Plaintiff Gonzalez signed up for the program in an attempt to mitigate the harms caused to him as a result of the Data Breach. Plaintiff Gonzalez has also purchased Experian credit monitoring at a cost of $34.99 per month, and Zandor Insurance at a cost of $145 per year.

181. Since the Data Breach, Plaintiff Gonzalez experienced identity fraud in the form of fraudulent financial accounts opened using his information. For example, in or around April 2022, Plaintiff Gonzalez received a Chime Visa Debit card that he had not applied for. Similarly, in April 2022, Plaintiff Gonzalez received notice of a Wells Fargo account that had fraudulently been opened using his PII. In July 2022, Plaintiff Gonzalez received an email notification from Capital One welcoming him to a Capital One 360 checking account that he had not opened. He also received notification of this incident from his Experian credit monitoring service, which advised him that his Social Security number had been used to open a Capital One 360 account.

182. As a result of the opening of these unauthorized accounts, Plaintiff Gonzalez was

required to contact the respective institutions to immediately close each of the accounts. Plaintiff Gonzalez also filed police reports about these fraudulent accounts. He believes the unauthorized accounts were opened as a result of the Data Breach given that these incidents occurred relatively soon after the Data Breach, and he had no other previous incidents like this.

183. In the past few months, Plaintiff Gonzalez has had to close three unauthorized financial accounts that were fraudulently opened using his PII. He spent considerable time in connection with closing these accounts, filing police reports, contacting the Social Security office and USAP Bank Services about the Data Breach and the subsequent identity theft, contacting the Federal Trade Commission and opening an account with identitytheft.gov, freezing his credit reports, and taking other actions in response to the Data Breach. Since learning of the Data Breach, Plaintiff Gonzalez has spent additional time reviewing his bank statements, credit cards, and credit monitoring reports.

184. Plaintiff Gonzalez estimates that he spent approximately 15 hours on the foregoing mitigation steps. Plaintiff spent this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

185. The Data Breach has caused Plaintiff Gonzalez to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

186. Plaintiff Gonzalez plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his bank, credit, and other accounts for any unauthorized activity.

187. Additionally, Plaintiff Gonzalez is very careful about sharing his PII. He has never

knowingly transmitted unencrypted PII over the internet or any other unsecured source.

188. Plaintiff Gonzalez stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

189. Plaintiff Gonzalez has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Robert Keach's Experience

190. As a condition to receiving loan services from his mortgage originator and servicers, whom he believes provided his PII to Pingora, Plaintiff Keach provided his PII to those mortgage originators and servicers, which was then provided to Pingora and entered into Pingora's database and maintained by Pingora.

191. Plaintiff Keach greatly values his privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Keach took reasonable steps to maintain the confidentiality of his PII.

192. Plaintiff Keach received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

193. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Keach faces, Defendant offered him a one subscription to a credit monitoring service. Plaintiff Keach has signed up for the program but does not believe it is sufficient to protect his

identity from the ongoing risks of theft he faces.

194. In December 2021, Plaintiff Keach experienced identity fraud in the form of an unauthorized $413 charge for a "security plan" through "Geek Squad"; he also received an unauthorized $451 bill for MacAfee service at approximately the same time; and in April 2022 he had an unauthorized charge of $284.99 from Norton LifeLock. He believes these unauthorized charges are a result of the Data Breach given that they occurred after the Data Breach and he had no other previous fraudulent charges.

195. Since learning of the Data Breach, Plaintiff Keach has spent additional time reviewing his bank statements, credit cards, and reviewing his emails for fraud alerts. Since April 2022, he has spent approximately one hour every day reviewing his bank, credit and debit card statements; and reviewing his emails for fraud alerts or otherwise suspicious fraudulent charges. Plaintiff spent this time at Pingora's direction. In the notice letter Plaintiff received, Pingora directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

196. Plaintiff Keach has experienced an increase of other spam calls, text messages and emails after the Data Breach.

197. Plaintiff Keach has received numerous emails showing transactions and invoices using his name and email, for which he is not responsible.

198. The Data Breach has caused Plaintiff Keach to suffer fear, anxiety, and stress, which has been compounded by the fact that Pingora has not been forthright with information about the Data Breach.

199. Plaintiff Keach plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository,

credit, and other accounts for any unauthorized activity.

200. Additionally, Plaintiff Keach is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

201. Plaintiff Keach stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

202. Plaintiff Keach has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Cindy Villanueva's Experience

203. Plaintiff Villanueva took out a loan to purchase her home. The original servicer was Dignified Home Loans. On or around December 6, 2019, Lakeview purchased the mortgage. As a condition to providing Plaintiff Villanueva loan services, Lakeview required access to Plaintiff Villanueva's PII, which it received and entered into its database to maintain.

204. Plaintiff Villanueva greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Villanueva took reasonable steps to maintain the confidentiality of her PII.

205. Plaintiff Villanueva received a letter dated March 17, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained her name, address, loan number, Social Security number, and, potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

206. Recognizing the present, immediate, and substantially increased risk of harm

Plaintiff Villanueva faces, Defendant offered her a one-year subscription to a credit monitoring service. Plaintiff Villanueva elected not to sign up for the credit monitoring.

207. Since October 2021, Plaintiff Villanueva noticed suspicious activities related to her bank account and has experienced fraud and identity theft. Specifically, she has had accounts opened under her name without authorization.

208. Several months ago, Plaintiff Villanueva discovered that an individual in Washington was attempting to purchase approximately $900 worth of electronics using her Amazon account. Then, in or around April of 2022, Plaintiff Villanueva was notified that a second subscription to Amazon was opened in her name and her account was charged $150. In May 2022, Plaintiff Villanueva received a call that Amazon suspected fraud related to her account when someone tried to purchase an iPhone using her account. Plaintiff Villanueva has since cancelled her Amazon account.

209. Plaintiff Villanueva has also experienced various unauthorized deductions continuously appearing in her checking account. For example, someone opened an Audible account using her debit card; she called to dispute the charge and the bank reversed the charges, but then the charge appeared again. Plaintiff Villanueva is going to cancel her debit card and request a new one to stop the unauthorized charges.

210. Plaintiff Villanueva spent time in connection with the Amazon account and debit card charges in response to the Data Breach.

211. Since learning of the Data Breach, Plaintiff Villanueva has spent additional time reviewing her bank statements and credit cards. Since April 2022, she has spent time every day reviewing her Amazon account information and bank, credit card and debit card statements, and/or going to her bank to initiate investigations into the unauthorized charges. Plaintiff Villanueva

spent this time at Lakeview's direction. In the notice letter Plaintiff Villanueva received, Lakeview directed Plaintiff Villanueva to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

212. Plaintiff Villanueva has experienced an increase of other spam calls, text messages and emails after the Data Breach.

213. The Data Breach has caused Plaintiff Villanueva to suffer fear, anxiety, and stress, which have been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

214. Plaintiff Villanueva plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

215. Additionally, Plaintiff Villanueva is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

216. Plaintiff Villanueva stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

217. Plaintiff Villanueva has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Deborah Hamilton's Experience

218. Plaintiff Hamilton used Lakeview's services when she took out a mortgage on her home. As a condition to receiving loan services from Lakeview, Plaintiff Hamilton provided her PII to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview.

219. Plaintiff Hamilton greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Hamilton took reasonable steps to maintain the confidentiality of her PII.

220. Plaintiff Hamilton received a letter dated March 18, 2022, from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

221. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Hamilton faces, Defendant offered her a one-year subscription to a credit monitoring service. Plaintiff Hamilton signed up for the program in an attempt to mitigate the harms caused to her as a result of the Data Breach. She has also purchased Lifelock identity theft protection at an annual cost of $339 per year.

222. In February 2022, Plaintiff Hamilton experienced identity fraud in the form of an unauthorized charge of $508 on her payment card. As a result, she was required to file a police report in response to the fraudulent charge. She believes the unauthorized charge is a result of the Data Breach given that it occurred relatively soon after the Data Breach, and she had no other previous fraudulent charges on her card.

223. Plaintiff Hamilton has been forced to spend time in connection with the unauthorized $508 charge, including time to file a police report and her other actions in response to the Data Breach.

224. Since learning of the Data Breach, Plaintiff Hamilton has spent additional time reviewing her bank statements and credit card statements. Plaintiff Hamilton estimates she has

spent approximately 10 hours responding to the Data Breach, including: reviewing her bank, credit, and debit card statements; attempting to obtain reimbursement of the $508 unauthorized charge; filing a police report about the fraudulent charge; and calling Lakeview to confirm the Data Breach and obtain further information. Plaintiff spent this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

225. The Data Breach has caused Plaintiff Hamilton to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

226. Plaintiff Hamilton plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her bank accounts, credit card accounts, and other personal information for any unauthorized activity.

227. Additionally, Plaintiff Hamilton is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

228. Plaintiff Hamilton stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

229. Plaintiff Hamilton has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Michael Kassem's Experience

230. Plaintiff Kassem used Pingora's services when his home mortgage was transferred to Pingora. As a condition to receiving loan services from Pingora, Plaintiff Kassem provided his

PII to Pingora, which was then entered into Pingora's database and maintained by Pingora.

231. Plaintiff Kassem greatly values his privacy and PII, especially when receiving loan and other financial services. Prior to the Data Breach, Plaintiff Kassem took reasonable steps to maintain the confidentiality of his PII.

232. Plaintiff Kassem received a letter dated April 6, 2022, from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

233. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Kassem faces, Defendant offered him a one-year subscription to a credit monitoring service. Plaintiff Kassem signed up for the program in an attempt to mitigate the harms caused to him as a result of the Data Breach. Plaintiff Kassem has also purchased Experian credit monitoring at a cost of $25 per month because he does not believe the program offered by Pingora is sufficient.

234. Since the Data Breach, Plaintiff Kassem experienced identity fraud in the form of unemployment fraud. In or around December 2021, Plaintiff Kassem was notified by the Georgia Department of Labor that someone had filed a fraudulent unemployment claim using his Social Security number. As a result, he was required to contact the Department of Labor concerning the fraudulent unemployment claim. He also filed a police report concerning the incident. Plaintiff Kassem had to drive to the police station to file the police report concerning fraudulent unemployment claim and estimates that he expended approximately $12 in gas money as a result. Plaintiff Kassem believes the fraudulent unemployment claim is a result of the Data Breach given that it occurred relatively soon after the Data Breach, and he has had no previous experiences of

fraudulent unemployment claims filed using his PII.

235. In the past few months, Plaintiff Kassem spent considerable time in connection with reporting the fraudulent unemployment claim and coordinating with the Department of Labor about the issue; filing a police report; researching and signing up for credit monitoring; placing a freeze on his credit reports; reviewing his bank statements, credit card statements, and credit monitoring reports; carefully reviewing his emails and other personal information for suspicious activity; and taking other steps in an attempt to mitigate the harm caused as a result of the Data Breach.

236. Plaintiff Kassem estimates that he has spent more than 20 hours on the foregoing mitigation steps. Plaintiff spent this time at Pingora's direction. In the notice letter Plaintiff received, Pingora directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

237. The Data Breach has caused Plaintiff Kassem to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Pingora has not been forthright with information about the Data Breach. The Data Breach and resulting identity theft have created stress that aggravated a back injury Plaintiff Kassem has, which has caused him considerable pain and lost time from work.

238. Plaintiff Kassem plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his bank, credit, and other accounts for any unauthorized activity.

239. Additionally, Plaintiff Kassem is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

240. Plaintiff Kassem stores any documents containing his PII in a safe and secure

location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

241. Plaintiff Kassem has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Beth Berg's Experience

242. Lakeview was the servicer for the residential mortgage on Plaintiff Berg's home. As a condition to receiving loan services from Lakeview, Plaintiff Berg provided her PII which was then entered into Lakeview's database and maintained by Lakeview.

243. Plaintiff Berg greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Berg took reasonable steps to maintain the confidentiality of her PII.

244. Plaintiff Berg received a letter dated March 21, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

245. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Berg faces, Defendant offered her a one-year subscription to a credit monitoring service.

246. Following the Data Breach, an unauthorized individual opened a checking account in Plaintiff Berg's name with Bank of America. On or about March 4, 2022, Plaintiff Berg received a Bank of America credit card in the mail containing her name. Shortly after, Plaintiff Berg received a letter from Bank of America asking her to call the bank as a result of "suspicious

activity." She later learned that someone obtained a cash advance in her name from Bank of America in the amount of $3,500 (which included an additional $200 in fees). This money was then deposited in the fraudulent checking account that was opened in her name. Plaintiff Berg had Bank of America freeze the checking account and close the credit card. She then contacted credit reporting agencies and was told that if she did not make a payment on the fraudulently obtained credit card, her credit score would decrease by approximately 25 to 100 points. As a result, Plaintiff Berg was forced to make a payment of $57 toward the credit card balance to avoid a negative impact on her credit score. This payment was never refunded.

247. In February 2022, an unauthorized actor filed a 2021 federal tax return in her name and fraudulently obtained an approximately $19,000 tax refund. The tax refund was deposited in an online bank account, which the unauthorized actor closed shortly thereafter. As a result, Plaintiff Berg was forced to file a corrected 2021 tax return, and she still has not received the tax refund owed to her.

248. Plaintiff Berg believes the fraud she suffered was a result of the Data Breach given the timing of the Data Breach, the types of data impacted, her diligence in maintaining PII in a secure manner, and the fact that, to her knowledge, she has not been the victim of another data breach since the occurrence of the Data Breach.

249. Plaintiff Berg was forced to spend significant time dealing with the fraudulent activity in her name, including approximately 80 phone calls with Bank of America, three trips to a local Bank of America branch (which required her to utilize her own vehicle and fuel), several communications with the IRS, and the filing of a police report. In total, Plaintiff Berg estimates that she spent over 100 hours dealing with the fraud committed against her.

250. The Data Breach has caused Plaintiff Berg to suffer fear, anxiety, and stress, which

has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

251. Plaintiff Berg plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

252. Additionally, Plaintiff Berg is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Berg stores any documents containing her PII in a safe and secure location or destroys the documents.

253. Plaintiff Berg has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Savannah Farley's Experience

254. Lakeview was the servicer for the residential mortgage on Plaintiff Farley's home. As a condition to receiving loan services from Lakeview, Plaintiff Farley provided her PII which was then entered into Lakeview's database and maintained by Lakeview.

255. Plaintiff Farley greatly values her privacy and PII, especially when receiving loan and other financial services. Prior to the Data Breach, Plaintiff Farley took reasonable steps to maintain the confidentiality of her PII.

256. Plaintiff Farley received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other

items regarding loan servicing.

257. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Farley faces, Defendant offered her a one-year subscription to a credit monitoring service. After receiving the letter, Plaintiff Farley signed up for this service.

258. In November of 2021, Plaintiff Farley experienced fraud in the form of approximately 80 unauthorized charges on her credit card. Plaintiff Farley learned of this fraud after attempting to use her credit card and having her purchase declined as a result of the fraudulent activity that she was previously unaware of. Because her card was frozen as a result of the unauthorized charges, Plaintiff Farley was unable to purchase Easter gifts for her children. After learning of the fraudulent charges, Plaintiff Farley spent several hours communicating with her bank via phone and email over the course of several weeks. Plaintiff Farley was also required to take time off of work to file a police report concerning the fraud on her account.

259. Plaintiff Farley believes the fraud was a result of the Data Breach given the timing, the type of data impacted, her diligence in maintaining her PII in a safe and secure manner, and the fact that, to her knowledge, she has never before been a victim of identity theft or fraud.

260. Following the fraudulent charges on her credit card, Plaintiff Farley purchased credit monitoring through Experian, which required an initial payment of approximately $30 and monthly charges thereafter of $5.99.

261. Since learning of the Data Breach, Plaintiff Farley has spent (and will continue to spend) additional time reviewing her bank statements and credit cards. Plaintiff Farley spent this time at Lakeview's direction. In the notice letter Plaintiff Farley received, Lakeview directed Plaintiff Farley to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

262. The Data Breach has caused Plaintiff Farley to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

263. Plaintiff Farley is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Farley stores any documents containing her PII in a safe and secure location or destroys the documents.

264. Plaintiff Farley has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Kristine Milewski's Experience

265. Plaintiff Milewski used Lakeview's services when she took out a mortgage on a rental property she owns. As a condition to receiving loan services from Lakeview, Plaintiff Milewski provided her PII to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview.

266. Plaintiff Milewski greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Milewski took reasonable steps to maintain the confidentiality of her PII.

267. Plaintiff Milewski received a letter dated April 4, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

268. Recognizing the present, immediate, and substantially increased risk of harm

Plaintiff Milewski faces, ffered her a subscription to a credit monitoring service. However, when Plaintiff Milewski tried to sign up for the program, she did not receive any response. As a result, she does not trust that Lakeview's chosen vendor can protect her information. Accordingly, Plaintiff Milewski enrolled in Norton LifeLock's identity theft prevention on May 16, 2022. She paid $419.86 for the service, which is billed annually.

269. On April 23, 2022, Plaintiff Milewski experienced identity fraud in the form of four credit card applications being submitted in her name. She first learned about the fraudulent activity on April 25, 2022, when she received a text message from Bank of America notifying her that she was approved for a credit card account. The other three applications were submitted to Barclays and American Express, and Plaintiff Milewski cancelled them before they arrived.

270. Additionally, Plaintiff Milewski experienced identity fraud when someone tried to obtain a personal loan in her name through CC Bank. The bank sent her an email on May 6, 2022, notifying her that the loan could not be completed without additional information. Further, on April 23, 2022, an unauthorized NerdWallet account was opened in her name. Someone opened the account and used it to access her credit and apply for multiple accounts at once. As a result, Plaintiff Milewski was required to close that account.

271. Since the Data Breach, Plaintiff Milewski also experienced identity fraud in the form of unauthorized charges on her Discover credit card. As a result, she was required to cancel the credit card.

272. Plaintiff Milewski believes each instance of identity fraud described above is a result of the Data Breach given that these events occurred relatively soon after the Data Breach. Plaintiff Milewski has spent over 60 hours addressing the fraud she has experienced since the Data Breach. She has filed a police report, made trips to Bank of America, filed a report with the FTC,

frozen credit accounts, cancelled credit cards, and spent countless hours speaking with account representatives.

273. Since learning of the Data Breach, Plaintiff Milewski has spent additional time reviewing her bank statements and credit cards. Plaintiff spent this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

274. The Data Breach has caused Plaintiff Milewski to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

275. Plaintiff Milewski plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

276. Additionally, Plaintiff Milewski is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

277. Plaintiff Milewski stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

278. Plaintiff Milewski has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Thomas Lapenter's Experience

279. Plaintiff Lapenter took out a loan in or around December 2018 to purchase his home. The original loan servicer was Mr. Cooper. He then refinanced with Rocket Mortgage,

from which Pingora purchased the mortgage. As a condition to providing Plaintiff Lapenter loan services, Pingora accessed his PII, which it then entered into its database and maintained.

280. Plaintiff Lapenter greatly values his privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Lapenter took reasonable steps to maintain the confidentiality of his PII.

281. Plaintiff Lapenter received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

282. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Lapenter faces, offered him a one-year subscription to a credit monitoring service. Plaintiff Lapenter did not sign up for the subscription. Plaintiff Lapenter instead signed up and paid for a monthly subscription for identity protection services through LifeLock in or about April or May 2022. He also paid to have his credit frozen.

283. Since October 2021, Plaintiff Lapenter has noticed suspicious bank activities and has had accounts opened under his name without authorization. Specifically, Plaintiff Lapenter learned that someone submitted a fraudulent loan application to his bank in his name when he received a loan denial letter in the mail then contacted his bank. Plaintiff Lapenter reasonably believes that this fraudulent loan application was related to the Data Breach because it occurred just after the Data Breach. Furthermore, the bank confirmed that the person used Plaintiff Lapenter's Social Security number on the application, which was exposed in the Data Breach.

284. Plaintiff Lapenter has spent approximately 20 hours contacting credit bureaus,

banks, freezing his credit, purchasing identity theft services that he trusts, and monitoring credit reports. Plaintiff Lapenter spent this time at Pingora's direction. In the notice letter Plaintiff Lapenter received, Pingora directed Plaintiff Lapenter to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

285. Plaintiff Lapenter plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

286. Additionally, Plaintiff Lapenter has spent $15 per month on the identity theft protection services, and he has also spent money to place credit freezes on his and his wife's credit reports. The credit freezes have made it more difficult for Plaintiff Lapenter to get loans for his business.

287. Plaintiff Lapenter has also experienced stress and anxiety about his credit and worries about debt being racked up in his name.

288. Plaintiff Lapenter is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

289. Plaintiff Lapenter stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

290. Plaintiff Lapenter has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Emily Holt's Experience

291. Plaintiff Holt used Lakeview's services when she took out a mortgage on her home.

As a condition to receiving loan services from Lakeview, Plaintiff Holt provided her PII to her original servicer. Lakeview then acquired the account, and her information. Plaintiff's PII was then entered into Lakeview's database and maintained by Lakeview.

292. Plaintiff Holt greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Holt took reasonable steps to maintain the confidentiality of her PII.

293. Plaintiff Holt received a letter dated June 10, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

294. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Holt faces, offered her a one-year subscription to a credit monitoring service.

295. Plaintiff Holt experienced identity fraud in the form of an unauthorized charge on her credit card. As a result, she was required to obtain a new credit card. She believes the unauthorized charges are a result of the Data Breach because they occurred relatively soon after the Data Breach, and she had no other previous fraudulent charges on her card.

296. Plaintiff Holt also discovered that her credit card points had been stolen from another credit card. As a result, she was required to obtain another new credit card.

297. Since learning of the Data Breach, Plaintiff Holt has spent additional time reviewing her bank statements and credit cards. Since February 2022, she has spent approximately ten hours reviewing her bank, credit and debit card statements and procuring new credit cards. Plaintiff Holt spent this time at Lakeview's direction. In the notice letter Plaintiff received,

Lakeview directed Plaintiff Holt to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

298. Plaintiff Holt has experienced an increase of spam calls, text messages and emails after the Data Breach.

299. The Data Breach has caused Plaintiff Holt to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

300. Plaintiff Holt plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

301. Additionally, Plaintiff Holt is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

302. Plaintiff Holt has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Hardik Sevak's Experience

303. Plaintiff Sevak used Lakeview's services when Lakeview acquired his mortgage on his home in Floral Park, New York. As a condition to receiving loan services from Lakeview, Plaintiff Sevak's PII was provided to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview.

304. Plaintiff Sevak greatly values his privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Sevak took reasonable steps to maintain the confidentiality of his PII.

305. Plaintiff Sevak received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his name, address, loan number, and Social Security number.

306. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Sevak faces, offered him a one-year subscription to a credit monitoring service.

307. In December 2021, Plaintiff Sevak experienced identity fraud in the form of an unauthorized third party attempting to secure financing in his name from Synchrony Bank. As a result, he contacted the bank to stop the fraudulent activity. He believes the unauthorized financing is a result of the Data Breach given that it occurred after the Data Breach, and he had no other previous fraudulent activity.

308. Since learning of the Data Breach Plaintiff Sevak has had to sign up for credit monitoring, identity theft and loss protection, including insurance against identity theft and identity restoration services. He now uses services provided by CreditKarma, Experian, and Transunion to protect his information.

309. Since learning of the Data Breach, Plaintiff Sevak has spent additional time reviewing his credit reports, bank statements and credit cards. Since the Data Breach, Plaintiff Sevak's information has been used by at least one unauthorized individual who attempted to open multiple fraudulent accounts and/or lines of credit in his name. As a result, he has spent approximately two hundred and fifty hours resolving issues related to these fraudulent accounts, including but not limited to: reviewing his bank, credit and debit card statements; reviewing his emails for credit alerts; and reviewing his credit reports for any unauthorized charges. Plaintiff Sevak spent this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff Sevak to spend time mitigating his losses by "reviewing your account statements

and free credit reports for unauthorized activity."

310. Plaintiff Sevak has experienced an increase of spam calls, text messages and emails after the Data Breach. The spam calls often included alarming personal details, which further contributed to Plaintiff Sevak's concern for his personal privacy and the safety of his identity. Moreover, following the Data Breach he received four phone calls from Experian regarding unauthorized individuals who were attempting to open lines of credit in his name.

311. The Data Breach has caused Plaintiff Sevak to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

312. Plaintiff Sevak plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

313. Additionally, Plaintiff Sevak is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

314. Plaintiff Sevak stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

315. Plaintiff Sevak has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff William Blando's Experience

316. Plaintiff Blando used Lakeview's services when he refinanced a home mortgage.

As a condition to receiving loan services from Lakeview, Plaintiff Blando provided his PII to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview.

317. Plaintiff Blando greatly values his privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Blando took reasonable steps to maintain the confidentiality of his PII.

318. Plaintiff Blando received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

319. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Blando faces, Defendant offered him a one-year subscription to a credit monitoring service. Plaintiff Blando has signed up for the program but does not believe it is sufficient to protect his identity from the ongoing risks of theft he faces.

320. In December 2021, Plaintiff Blando experienced identity fraud in the form of an unauthorized loan taken out in his name from Mountain Summit Financial Inc. As a result, he was required to contact the police and file a report, contact Mountain Summit Financial Inc., prove his identity, and explain that he did not take out a loan. To do so, he was required to execute a notarized affidavit. He believes the unauthorized loan is a result of the Data Breach given that it occurred after the Data Breach, and he had no other previous fraudulent activity.

321. Plaintiff Blando spent time in connection with addressing this fraudulent loan including having to drive to and from both the police station and his bank, equaling mileage of 20 miles and approximately 8 hours of lost time.

322. Since learning of the Data Breach, Plaintiff Blando has spent additional time reviewing his bank statements, debit cards, credit reports, and credit cards. Since December 2021, he has spent approximately eighteen hours reviewing his bank, credit and debit card statements; procuring a police report; communicating with Mountain Summit Financial; drafting and executing an affidavit; and going to his bank to initiate investigations into the unauthorized loan. Plaintiff spent this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

323. Plaintiff Blando has experienced an increase of spam calls, text messages and emails after the Data Breach.

324. Plaintiff Blando has received numerous emails showing transactions and invoices using his name and email, for which he is not responsible.

325. The Data Breach has caused Plaintiff Blando to suffer significant fear, embarrassment, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

326. The Data Breach has also caused Plaintiff Blando to suffer significant personal impact in the form of the unauthorized loan taken out in his name causing arguments with his daughter.

327. Plaintiff Blando plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

328. Additionally, Plaintiff Blando is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

329. Plaintiff Blando stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

330. Plaintiff Blando has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Julie Abraham's Experience

331. Plaintiff used Pingora's services when she and her husband acquired a mortgage on their home. As a condition to receiving loan services from Pingora, Plaintiff provided her PII to Pingora which was then entered into Pingora's database and maintained by Pingora.

332. Plaintiff greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of her PII.

333. Plaintiff received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

334. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff faces, Defendant offered her a one-year subscription to a credit monitoring service.

335. Plaintiff and her husband experienced identity fraud in the form of unauthorized withdrawals from their bank account. As a result, they were required to change their account details and have since closed the account. Soon after, Plaintiff experienced unauthorized withdrawals

from their account held with another financial institution and received unauthorized charges for a fraudulent account that was created in their names. Plaintiff believes that the unauthorized withdrawals and charges were a result of the Data Breach because they occurred relatively soon after the Data Breach, and they had no other previous fraudulent charges.

336. Since learning of the Data Breach, Plaintiff has spent additional time reviewing her bank statements and credit cards. Plaintiff spent this time at Pingora's direction. In the notice letter Plaintiff received, Pingora directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

337. Plaintiff has experienced an increase of spam calls, text messages and emails after the Data Breach.

338. Plaintiff plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

339. Additionally, Plaintiff is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

340. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Peter Wojciechowski's Experience

341. Plaintiff Wojciechowski took out a loan to purchase his home through Pulte Homes, a home builder. Lakeview purchased the mortgage two months later, in or around August 2021. As a condition to providing Plaintiff Wojciechowski loan services, Lakeview required access to his PII, which it then entered into its database and maintained.

342. Plaintiff Wojciechowski greatly values his privacy and PII, especially when

receiving loan and financial services. Prior to the Data Breach, Plaintiff Wojciechowski took reasonable steps to maintain the confidentiality of his PII.

343. Plaintiff Wojciechowski received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

344. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Wojciechowski faces, Defendant offered him a one-year subscription to a credit monitoring service. Plaintiff Wojciechowski signed up for the one-year subscription.

345. Plaintiff Wojciechowski experienced a fraud attempt on his United Services Automobile Association ("USAA") account where his name, date of birth, routing, and checking account information were compromised.

346. Since October 2021, Plaintiff Wojciechowski has noticed suspicious bank activities. Specifically, he incurred a fraudulent Apple Store charge of $708 on or around May 18, 2022.[38] Plaintiff Wojciechowski found out about the unauthorized activity by checking his bank accounts every morning. In order to obtain the money back, Plaintiff Wojciechowski spent approximately 12 hours on the phone with USAA and they eventually reversed the charges.

347. Plaintiff Wojciechowski spent approximately 12 hours with USAA related to the fraudulent ACH transaction, six hours freezing his credit, and approximately 70 hours actively monitoring his bank and credit card account information. Plaintiff Wojciechowski spent this time at Lakeview's direction. In the notice letter Plaintiff Wojciechowski received, Lakeview directed

[38] The payment was processed through a form of electronic bank transaction made using a network called an Automated Clearing House ("ACH").

Plaintiff Wojciechowski to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

348. Plaintiff Wojciechowski plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

349. Additionally, Plaintiff Wojciechowski is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

350. Plaintiff Wojciechowski stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

351. Plaintiff Wojciechowski has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Kimberley Rowton's Experience

352. Plaintiff Rowton used Pingora's services when her home mortgage was transferred to Pingora. As a condition to receiving loan services from Pingora, Plaintiff Rowton provided her PII to Pingora, which was then entered into Pingora's database and maintained by Pingora.

353. Plaintiff Rowton greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Rowton took reasonable steps to maintain the confidentiality of her PII.

354. Plaintiff Rowton received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained her name, address, loan number, Social Security number, and

potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

355. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Rowton faces, Defendant offered her a one-year subscription to a credit monitoring service. Plaintiff Rowton signed up for the program in an attempt to mitigate the harms caused to her as a result of the Data Breach.

356. Since the dates of the Data Breach, Plaintiff Rowton experienced identity fraud in the form of fraudulent transfers from her financial account. In January 2022, Plaintiff Rowton became aware that someone had used her PII to access one of her investment accounts and fraudulently transferred more than $11,000 from it. As a result, Plaintiff Rowton contacted the investment institution to try to receive reimbursement and has filed a complaint with the FBI about the incident. To date, Plaintiff Rowton has not received reimbursement of the funds she lost due to the Data Breach. Plaintiff Rowton believes the fraudulent transfer of funds from her account using her PII is a result of the Data Breach given that it occurred relatively soon after the Data Breach and that she had never experienced a fraudulent financial transfer before.

357. In addition to the more than $11,000 in funds that have been stolen from Plaintiff Rowton, she has also spent considerable time as a result of the Data Breach. In particular, Plaintiff Rowton estimates she has spent more than 40 hours responding to the Data Breach, including multiple attempts to receive reimbursement for the funds transferred from her account; filing a report with the FBI about the fraudulent account transfer; signing up for credit monitoring; freezing her credit reports; reviewing her bank statements and other account statements; reviewing her credit monitoring reports; closely monitoring all activity involving her PII; and taking other actions in response to the Data Breach.

358. Plaintiff spent this time at Pingora's direction. Indeed, in the notice letter Plaintiff received, Pingora directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

359. The Data Breach has caused Plaintiff Rowton to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Pingora has not been forthright with information about the Data Breach. Among other things, the Data Breach has caused Plaintiff Rowton to experience stress and anxiety. Plaintiff Rowton had finally retired in August 2021 and is now concerned about her ability to provide for herself in the aftermath of having lost a considerable portion of her retirement savings.

360. Plaintiff Rowton plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial statements and other personal information for any unauthorized or fraudulent activity.

361. Additionally, Plaintiff Rowton is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

362. Plaintiff Rowton stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

363. Plaintiff Rowton has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Dylan Normile's Experience

364. Plaintiff Normile used Lakeview's services when he refinanced his home mortgage using Lakeview. As a condition to receiving loan services from Lakeview, Plaintiff Normile

provided his PII to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview.

365. Plaintiff Normile greatly values his privacy and PII, especially when receiving loan and other financial services. Prior to the Data Breach, Plaintiff Normile took reasonable steps to maintain the confidentiality of his PII.

366. Plaintiff Normile received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

367. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Normile faces, Defendant offered him a one-year subscription to a credit monitoring service.

368. Since the Data Breach, Plaintiff Normile experienced identity fraud in the form of a fraudulent charge of approximately $25 on his debit card. As a result, he was required to contact his bank to report the fraudulent charge. He believes the unauthorized charge is a result of the Data Breach given that it occurred relatively soon after the Data Breach, and he has had no other previous fraudulent charges on his debit charge.

369. In the past few months, Plaintiff Normile spent time in connection with reporting the fraudulent charge to his bank; reviewing his bank statements, credit card statements, and credit reports; reviewing his emails and other personal information for suspicious activity; and taking other steps in an attempt to mitigate the harm caused as a result of the Data Breach.

370. Plaintiff Normile estimates that he has spent more than three hours on the foregoing

mitigation steps. Plaintiff spent this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

371. The Data Breach has caused Plaintiff Normile to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

372. Plaintiff Normile plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his bank, credit, and other accounts for any unauthorized activity.

373. Additionally, Plaintiff Normile is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

374. Plaintiff Normile stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

375. Plaintiff Normile has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Jessica Valente-Brodrick's Experience

376. Plaintiff Valente-Brodrick used Lakeview's services when she and her husband took out a mortgage on their home. As a condition to receiving loan services from Lakeview, Plaintiff Valente-Brodrick and her husband provided PII to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview.

377. Plaintiff Valente-Brodrick greatly values her privacy and PII, especially when

receiving loan and financial services. Prior to the Data Breach, Plaintiff Valente-Brodrick took reasonable steps to maintain the confidentiality of her PII.

378. Plaintiff Valente-Brodrick's husband received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

379. Recognizing the present, immediate, and substantially increased risk of harm she and her husband face, the Brodricks purchased identity theft monitoring prevention from Norton LifeLock which costs $299.88 annually.

380. In recent months, Plaintiff Valente-Brodrick has experienced identity fraud in the form of an unauthorized Wells Fargo account being opened in her name. She has also experienced several phishing attempts and suspicious activity, including receiving fake order and shipping alerts. She believes these events are a result of the Data Breach given that they occurred relatively soon after the Data Breach, and she had no other previous fraudulent activity or persistent phishing attempts prior to the Data Breach.

381. Since learning of the Data Breach, Plaintiff Valente-Brodrick has spent additional time reviewing her bank statements and credit cards. Moreover, Plaintiff spent this time at Lakeview's direction. Indeed, in the notice letter her husband received, Lakeview directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

382. Plaintiff Valente-Brodrick has experienced an increase of other spam calls, text messages and emails after the Data Breach.

383. The Data Breach has caused Plaintiff Valente-Brodrick to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

384. Plaintiff Valente-Brodrick plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

385. Additionally, Plaintiff Valente-Brodrick is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

386. Plaintiff Valente-Brodrick stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

387. Plaintiff Valente-Brodrick has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff April Burnett's Experience

388. Plaintiff Burnett used Lakeview's services when her home mortgage was transferred to Lakeview. As a condition to receiving loan services from Lakeview, Plaintiff Burnett provided her PII to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview.

389. Plaintiff Burnett greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Burnett took reasonable steps to maintain the confidentiality of her PII.

390. Plaintiff Burnett received a letter dated April 4, 2022 from Defendant Lakeview

concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

391. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Burnett faces, Defendant offered her a one-year subscription to a credit monitoring service. However, Plaintiff Burnett has not signed up for the program, as she does not trust that Lakeview's chosen vendor can protect her information. Instead, Plaintiff Burnett is using credit monitoring from a service she trusts.

392. In April 2022, Plaintiff Burnett experienced identity fraud in the form of a fraudulent tax return that was being filed using her information. As a result, she was required to contact her tax return service provider to stop the fraudulent tax return from being filed. Plaintiff Burnett was further required to contact her lender and her bank to advise them of the situation because she was in the process of closing on a house when the fraudulent tax filing was attempted. Plaintiff Burnett was even required to drive to her bank to implement additional security measures on her account and to obtain a letter from her bank advising that if any fraudulent transactions occurred, the mortgage underwriter for the home she was closing on would be notified. Plaintiff Burnett believes the fraudulent tax return using her information is a result of the Data Breach given that it occurred relatively soon after the Data Breach and that she had never before experienced an instance of a fraudulently filed tax return.

393. Plaintiff spent considerable time in connection with stopping the filing of the fraudulent tax return, notifying relevant financial institutions, and taking other actions in response to the fraudulent tax return. Plaintiff Burnett estimates that she spent approximately five hours on

these efforts.

394. Since learning of the Data Breach, Plaintiff Burnett has spent additional time reviewing her bank statements and other account statements. Since April 2022, she has spent approximately one hour every day reviewing her bank account information and other personal information. Plaintiff Burnett also spent time contacting Lakeview in an attempt to learn additional information about the Data Breach and her resulting exposure. Plaintiff spent this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

395. The Data Breach has caused Plaintiff Burnett to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach. Among other things, the Data Breach has caused Plaintiff Burnett to experience anxiety about whether she would be able to close on the house she was in the process of buying.

396. Plaintiff Burnett plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her tax information, bank statements, and other personal information for any unauthorized or fraudulent activity.

397. Additionally, Plaintiff Burnett is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

398. Plaintiff Burnett stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

399. Plaintiff Burnett has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Denise Scott's Experience

400. Plaintiff Scott used Lakeview's services when she took out a mortgage on her home. As a condition to receiving loan services from Lakeview, Plaintiff Scott provided her PII to Lakeview which was then entered into Lakeview's database and maintained by Lakeview.

401. Plaintiff Scott greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Scott took reasonable steps to maintain the confidentiality of her PII.

402. Plaintiff Scott received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

403. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Scott faces, Defendant offered her a one-year subscription to a credit monitoring service.

404. In January 2022, Plaintiff Scott experienced identity fraud when someone fraudulently accessed her mortgage account and altered her payment settings. As a result, Plaintiff Scott received a letter from Lakeview that they were foreclosing on her home. Additionally, Plaintiff Scott incurred late fees totaling $213.80.

405. In February 2022, Plaintiff Scott experienced additional identity fraud when someone attempted to charge $790 on her American Express credit card. As a result, she closed

this card and had to replace it.

406. Since learning of the Data Breach, Plaintiff Scott has spent additional time reviewing her bank statements and credit cards. Since January 2022, she has spent approximately forty hours dealing with the fraud attempts and attempting to mitigate the impact of the Data Breach. Moreover, Plaintiff spent this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

407. The Data Breach has caused Plaintiff Scott to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

408. Plaintiff Scott plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

409. Additionally, Plaintiff Scott is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

410. Plaintiff Scott stores any documents containing her PII in a safe and secure location or destroys the documents.

411. Plaintiff Scott has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, and is protected and safeguarded from future breaches.

Plaintiff Julia Franke's Experience

412. Lakeview was the servicer for the residential mortgage on Plaintiff Franke's home. As a condition to receiving loan services from Pingora, Plaintiff Franke provided her PII to

Pingora, which was then entered into Pingora's database and maintained by Pingora.

413. Plaintiff Franke greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Franke took reasonable steps to maintain the confidentiality of her PII.

414. Plaintiff Franke received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

415. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Franke faces, Defendant offered her a one-year subscription to a credit monitoring service.

416. In December 2021, Plaintiff Franke received a fraudulent $100 charge for a "Home Warranty" on her credit card. Unsure of whether the charge was legitimate, Plaintiff Franke reached out to the company that she has her home warranty with. The company informed her that the charge was not legitimate and that she should report it to her bank as fraud. After reporting the incident to her bank, Plaintiff Franke's credit cards were cancelled and had to be reissued. It took over a month for the bank to resolve the fraudulent activity associated with Plaintiff Franke's account, during which time she was required to spend several hours coordinating with her bank. Plaintiff Franke believes that the fraudulent charge was a result of the Data Breach given that it occurred relatively soon after the Data Breach, and she had no other previous fraudulent charges on that card.

417. Since learning of the Data Breach, Plaintiff Franke has spent additional time responding to the data breach and reviewing her financial accounts. Plaintiff Franke spent this time

at Pingora's direction. Indeed, in the notice letter Plaintiff received, Pingora directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

418. Plaintiff Franke has experienced an increase of other spam calls, text messages and emails after the Data Breach.

419. The Data Breach has caused Plaintiff Franke to suffer fear, anxiety, and stress, which has been compounded by the fact that Pingora has not been forthright with information about the Data Breach.

420. Plaintiff Franke plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

421. Additionally, Plaintiff Franke is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

422. Plaintiff Franke stores any documents containing her PII in a safe and secure location or destroys the documents.

423. Plaintiff Franke has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiffs Ashley and Richard Cashon's Experience

424. Plaintiffs Ashley and Richard Cashon used Lakeview's services when they refinanced a mortgage on their home. As a condition to receiving loan services from Lakeview, Plaintiffs provided their PII to Lakeview which was then entered into Lakeview's database and maintained by Lakeview.

425. Plaintiffs greatly value their privacy and PII, especially when receiving loan and other financial services. Prior to the Data Breach, Plaintiffs took reasonable steps to maintain the confidentiality of their PII.

426. Plaintiffs received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained their name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

427. Recognizing the present, immediate, and substantially increased risk of harm Plaintiffs face, Defendant offered them a one-year subscription to a credit monitoring service.

428. In May 2022, Plaintiffs experienced identity fraud in the form of an unauthorized charges on their debit card for their checking account. As a result, they were required to obtain a new card. They believe that the unauthorized charges on their card was a result of the Data Breach because it occurred relatively after the Data Breach, and they had no other previous fraudulent charges.

429. Since learning of the Data Breach, Plaintiffs have spent additional time reviewing their bank statements and credit card accounts. Moreover, Plaintiffs spent this time at Lakeview's direction. Indeed, in the notice letter Plaintiffs received, Lakeview directed Plaintiffs to spend time mitigating their losses by "reviewing your account statements and free credit reports for unauthorized activity."

430. Plaintiffs have experienced an increase of spam calls, text messages and emails after the Data Breach.

431. Plaintiffs plan to take additional time-consuming, necessary steps to help mitigate

the harm caused by the Data Breach, including continually reviewing their depository, credit, and other accounts for any unauthorized activity.

432. Additionally, Plaintiffs are very careful about sharing her PII. They have never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

433. Plaintiffs have a continuing interest in ensuring that their PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Nilsa Misencik's Experience

434. Plaintiff Misencik used Lakeview's services when she took out a mortgage on her home. As a condition to receiving loan services from Lakeview, Plaintiff Misencik provided her PII to Lakeview which was then entered into Lakeview's database and maintained by Lakeview.

435. Plaintiff Misencik greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Misencik took reasonable steps to maintain the confidentiality of her PII.

436. Plaintiff Misencik received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

437. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Misencik faces, Defendant offered her a one-year subscription to a credit monitoring service.

438. In February 2022, Plaintiff Misencik experienced identity fraud in the form of an

unauthorized application and denial of a credit card from Bank of America. She believes the credit card application is a result of the Data Breach because it occurred relatively soon after the Data Breach.

439. Plaintiff Misencik also received a bill for an unauthorized purchase of a home appliance. Upon calling the biller, Plaintiff Misencik learned that the appliance seller had her date of birth, full name, social security number, address and phone number—information compromised in the Data Breach.

440. Since learning of the Data Breach, Plaintiff Misencik has spent additional time reviewing her bank statements and credit cards. Since February 2022, she has spent several hours reviewing her bank, credit and debit card statements; dealing with fraudulent purchases; and spending time on the phone dealing with the unauthorized credit card application and other unauthorized charges. Plaintiff spent this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

441. The Data Breach has caused Plaintiff Misencik to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

442. Plaintiff Misencik plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

443. Additionally, Plaintiff Misencik is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

444. Plaintiff Misencik has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Robert Martin's Experience

445. Plaintiff Martin used Lakeview's services when he took out a mortgage on his home and when he refinanced his home. As a condition to receiving loan services from Lakeview, Plaintiff Martin provided his PII to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview.

446. Plaintiff Martin greatly values his privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Martin took reasonable steps to maintain the confidentiality of his PII.

447. Plaintiff Martin received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

448. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Martin faces, Defendant offered him a one-year subscription to a credit monitoring service which Plaintiff Martin immediately enrolled in. Additionally, Plaintiff Martin has utilized Equifax's fraud alerts for several years and also monitors his credit using free services provided by Experian.

449. In May 2022, Plaintiff Martin experienced identity fraud in the form of unauthorized charges on his credit card account. Chase Bank alerted Plaintiff Martin of the

fraudulent activity in May 2022. He believes the unauthorized charges are a result of the Data Breach because they occurred relatively soon after the Data Breach. As a result of this fraudulent activity, Plaintiff Martin was required to spend time speaking with customer service representatives in order to dispute the fraudulent charges and have them removed from his account.

450. Since learning of the Data Breach, Plaintiff Martin has spent additional time reviewing his bank statements and credit cards, and he checks each of his accounts on a regular basis. Plaintiff spent this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

451. The Data Breach has caused Plaintiff Martin to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

452. Plaintiff Martin plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

453. Additionally, Plaintiff Martin is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

454. Plaintiff Martin stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

455. Plaintiff Martin has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Christopher Spark's Experience

456. Plaintiff Sparks used Lakeview's services when he took out a mortgage on his home. As a condition to receiving loan services from Lakeview, Plaintiff Sparks provided his PII to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview.

457. Plaintiff Sparks greatly values his privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Sparks took reasonable steps to maintain the confidentiality of his PII.

458. Plaintiff Sparks received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

459. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Sparks faces, Defendant offered him a subscription to a credit monitoring service. However, Plaintiff Sparks has not signed up for the program, as he does not trust that Lakeview's chosen vendor can protect his information. Plaintiff Sparks is enrolled in credit monitoring alerts through his bank account with Capital One and receives additional identity theft monitoring services from Allstate.

460. In April 2022, Plaintiff Sparks experienced identity fraud in the form of a checking account and an unauthorized credit card account being opened in his name. Plaintiff Sparks did not learn about this fraudulent activity until he received a letter from Bank of America in May 2022. He believes the unauthorized account openings are a result of the Data Breach because they occurred relatively soon after the Data Breach. As a result of this fraudulent activity, Plaintiff

Sparks' work schedule was interrupted, and he was required to spend several hours speaking with customer service representatives in order to dispute the charges and close the fraudulent accounts.

461. Since learning of the Data Breach, Plaintiff Sparks has spent additional time reviewing his bank statements and credit cards, and he checks each of his accounts on a daily basis. Plaintiff spent this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

462. The Data Breach has caused Plaintiff Sparks to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

463. Plaintiff Sparks plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

464. Additionally, Plaintiff Sparks is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

465. Plaintiff Sparks stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

466. Plaintiff Sparks has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff David Kraus' Experience

467. Plaintiff Kraus used Pingora's services when he took out a mortgage on his home.

As a condition to receiving loan services from Pingora, Plaintiff Kraus provided his PII to Pingora which was then entered into Pingora's database and maintained by Pingora.

468. Plaintiff Kraus greatly values his privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Kraus took reasonable steps to maintain the confidentiality of his PII.

469. Plaintiff Krauss received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

470. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Kraus faces, Defendant offered him a one-year subscription to a credit monitoring service.

471. In April 2022, Plaintiff Kraus experienced identity fraud in the form of unauthorized charges on his credit card in the amount of $250, and $2,563. As a result, he was required to obtain a new card. He believes the unauthorized charges on his debit card are a result of the Data Breach because they occurred relatively soon after the Data Breach, and he had no other previous fraudulent charges on his card.

472. Around that same time, Plaintiff Kraus' computer was hacked and held hostage by a computer scam.

473. Since learning of the Data Breach, Plaintiff Kraus has spent additional time reviewing his bank statements and credit cards. Since February 2022, he has spent approximately 40 hours in total, reviewing his bank, credit and debit card statements; procuring a new credit card; speaking with government officials; and speaking with bank employees. Plaintiff spent this time

at Pingora's direction. In the notice letter Plaintiff received, Pingora directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

474. Plaintiff Kraus has experienced an increase of other spam calls, text messages and emails after the Data Breach.

475. The Data Breach has caused Plaintiff Kraus to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

476. Plaintiff Kraus plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

477. Additionally, Plaintiff Kraus is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

478. Plaintiff Kraus has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, and is protected and safeguarded from future breaches.

Plaintiff John McMahon's Experience

479. Plaintiff McMahon used Lakeview's services when he took out a mortgage on his home. As a condition to receiving loan services from Lakeview, Plaintiff McMahon provided his PII to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview.

480. Plaintiff McMahon greatly values his privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff McMahon took reasonable steps to maintain the confidentiality of his PII.

481. Plaintiff McMahon received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

482. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff McMahon faces, Defendant offered him a one-year subscription to a credit monitoring service. After receiving the letter, Plaintiff McMahon signed up for this service.

483. On January 25, 2022, Plaintiff McMahon received a notification from the credit monitoring service that he maintained through Discover informing him that his Social Security number was "compromised." The alert further stated: "We have located your Social Security number on a Dark Web site." Plaintiff believes that this was a result of the Data Breach given the timing of the notification, his diligence in storing and maintaining his PII in a secure manner, and the fact that, to his knowledge, he has not been the subject of any other data breaches impacting his Social Security number.

484. As a result of the Data Breach and notification that his PII is on the dark web, Plaintiff McMahon was forced to cancel all of his credit cards and have them reissued, which took significant time.

485. Since learning of the Data Breach, Plaintiff McMahon has suffered a further loss of time (and continues to spend a considerable amount of time) on issues related to this Data Breach, such as monitoring accounts and credit scores. He also spent considerable time implementing an alert with one of the major credit bureaus, and intends to spend time taking additional steps to protect his PII. Plaintiff spent this time at Lakeview's direction. In the notice letter Plaintiff

McMahon received, Lakeview directed Plaintiff McMahon to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

486. The Data Breach has caused Plaintiff McMahon to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

487. Plaintiff McMahon is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

488. Plaintiff McMahon stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

489. Plaintiff McMahon has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Shannon Thomas' Experience

490. Plaintiff Thomas took out a mortgage loan for property in Ohio. For all times relevant to this Complaint, Defendant Lakeview was the servicer of Plaintiff Thomas' mortgage loan. As a condition to providing Plaintiff Thomas loan services, Lakeview accessed Plaintiff Thomas' PII, which it then entered into its database and maintained.

491. Plaintiff Thomas provided Defendant Lakeview with significant personal, income, and financial information that Defendant Lakeview was able to acquire and to supplement by obtaining credit reports and banking information from third parties.

492. Plaintiff Thomas greatly values her privacy and PII, especially when receiving loan and financial services. Plaintiff Thomas takes reasonable steps to maintain the confidentiality of

her PII.

493. Plaintiff Thomas received a letter on or around March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

494. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Thomas faces, Defendant Lakeview offered her a one-year subscription to a credit monitoring service.

495. Since October 2021, as a direct result of the Data Breach, Plaintiff Thomas has already had to spend time and energy protecting and monitoring her identity and credit. Plaintiff Thomas spent time reviewing bank accounts and statements, changing passwords related to her business and personal accounts, reviewing her credit reports from all three credit bureaus, and she will have to spend additional time and energy in the future continuing to monitor and protect her identity and credit. Plaintiff Thomas spent this time at Lakeview's direction. In the notice letter Plaintiff Thomas received, Defendant Lakeview directed Plaintiff Thomas to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

496. As a direct result of the Data Breach, Plaintiff has suffered anxiety, emotional distress, and loss of privacy.

497. Additionally, Plaintiff Thomas has also spent money out of pocket to address the Data Breach and purchased LifeLock Advantage, an identity theft protection product, for $15.99 per month.

498. Plaintiff Thomas has experienced an increase of spam calls, text messages and emails after the Data Breach.

499. Plaintiff Thomas plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

500. Additionally, Plaintiff Thomas is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

501. Plaintiff Thomas stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

502. Plaintiff Thomas has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants Lakeview's possession, is protected and safeguarded from future breaches.

Plaintiff Mathew Myers' Experience

503. Plaintiff Myers used Lakeview's services when Lakeview acquired his mortgage on his home in August 2019. As a condition to receiving loan services from Lakeview, Plaintiff Myers' PII was provided to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview.

504. Plaintiff Myers greatly values his privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Myers took reasonable steps to maintain the confidentiality of his PII.

505. Plaintiff Myers received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on

Lakeview's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

506. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Myers faces, Defendant offered him a one-year subscription to a credit monitoring service. However, Plaintiff Myers has not signed up for the program, as he does not trust that Lakeview's chosen vendor can protect his information. Plaintiff Myers instead signed up for credit monitoring and identity theft protection services through LifeLock, Credit Karma, Transunion, and Norton in order to protect his information. These services cost Plaintiff Myers $16 per month.

507. Since learning of the Data Breach, Plaintiff Myers has spent additional time reviewing his credit reports, bank statements and credit cards. Since April 2022, he has spent approximately one to two hours every day reviewing his bank, credit and debit card statements; reviewing his emails for credit alerts; and reviewing his credit reports for any unauthorized charges. Moreover, Plaintiff spent this time at Lakeview's direction. Indeed, in the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

508. Plaintiff Myers has experienced an increase of other spam calls, text messages and emails after the Data Breach.

509. As a result of the Data Breach Plaintiff Myers had to sign up for, and pay for, the service "Nomorobo" to address the influx of spam calls, at a cost to him of $19.99 per year.

510. The Data Breach has caused Plaintiff Myers to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

511. Plaintiff Myers plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

512. Additionally, Plaintiff Myers is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

513. Plaintiff Myers stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

514. Plaintiff Myers has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Jay Saporta's Experience

515. Plaintiff Saporta used Pingora's services when he took out a mortgage on his home. As a condition to receiving loan services from Pingora, Plaintiff Saporta provided his PII to Pingora, which was then entered into Pingora's database and maintained by Pingora.

516. Plaintiff Saporta greatly values his privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Saporta took reasonable steps to maintain the confidentiality of his PII.

517. Plaintiff Saporta received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

518. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Saporta faces, Defendant offered him a one-year subscription to a credit monitoring service.

519. In or around May of 2022, Plaintiff Saporta learned that his information was published on the dark web. He first learned about this fraudulent activity when he received an alert from Turbo Tax in conjunction with a free identity theft prevention subscription he has had for several years.

520. Since learning of the Data Breach, Plaintiff Saporta made reasonable efforts to mitigate the impact of the Data Breach—at Defendant's direction—including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; placing a fraud alert on his credit report with all 3 credit report agencies due to the Data Breach, which costs him approximately $15.00 per month; and reviewing the credit monitoring service offered by Pingora. Plaintiff Saporta has spent several hours dealing with the fallout from this Data Breach, valuable time Plaintiff Jay Saporta otherwise would have spent on other activities, including but not limited to work and/or recreation.

521. The Data Breach has caused Plaintiff Saporta to suffer fear, anxiety, and stress, which has been compounded by the fact that Pingora has not been forthright with information about the Data Breach.

522. Plaintiff Saporta plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

523. Additionally, Plaintiff Saporta is very careful about sharing his PII. He has never

knowingly transmitted unencrypted PII over the internet or any other unsecured source.

524. Plaintiff Saporta stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

525. Plaintiff Saporta has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Derek Crenshaw's Experience

526. Plaintiff Crenshaw used Lakeview's services when he took out a mortgage on his home. As a condition to receiving loan services from Lakeview, Plaintiff Crenshaw provided his PII to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview.

527. Plaintiff Crenshaw greatly values his privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Crenshaw took reasonable steps to maintain the confidentiality of his PII.

528. Plaintiff Crenshaw received a letter dated March 17, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

529. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Crenshaw faces, Defendant offered him a one-year subscription to a credit monitoring service.

530. Since learning of the Data Breach, Plaintiff Crenshaw has spent additional time

reviewing his bank statements and credit cards. Since March 2022, he has spent approximately ten additional minutes every day reviewing his bank, credit and debit card statements. Plaintiff spent this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

531. Plaintiff Crenshaw has experienced an increase of spam calls, text messages and emails after the Data Breach.

532. As a result of this Data Breach leading to an increase in spam calls and text messages, Plaintiff Crenshaw has had substantial interference with his work as a salesperson. As part of his job he is responsible for answering every phone call and reading every text message, without the ability to screen phone calls and text messages as likely spam. Plaintiff Crenshaw has had to waste substantial time, time he otherwise would have spent working and speaking with clients and customers, answering these spam calls and reading these spam text messages. Additionally, Plaintiff Crenshaw has missed client and customer phone calls as a result of being on the phone with these spam calls.

533. The Data Breach has caused Plaintiff Crenshaw to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

534. Plaintiff Crenshaw plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, and other accounts for any unauthorized activity.

535. Additionally, Plaintiff Crenshaw is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

536. Plaintiff Crenshaw stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for her various online accounts.

537. Plaintiff Crenshaw has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiffs' Injuries and Damages

538. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members are presently experiencing and will continue experiencing actual harm from fraud and identity theft.

539. Plaintiffs and Class Members are presently experiencing substantial risk of out-of-pocket fraud losses, such as loans opened in their names, tax return fraud, utility bills opened in their names, and similar identity theft.

540. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

541. Plaintiffs and Class Members are also incurring and may continue incurring out-of-pocket costs for protective measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in lieu of the inadequate monitoring offered by Defendants), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

542. Plaintiffs and Class Members also suffered a loss of value of their PII when it was acquired by the cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

543. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendants were intended to be used by Defendants to fund adequate security of Defendants' computer property and protect Plaintiffs' and Class Members' PII. Thus, Plaintiffs and the Class Members did not get what they paid for.

544. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse. Indeed, Defendants' own notice of data breach provides instructions to Plaintiffs and Class Members about all the time that they will need to spend monitor their own accounts and statements received from healthcare providers and health insurance plans.

545. Plaintiffs and Class Members have suffered actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security number, medical insurance accounts, bank accounts, payment card statements, and credit reports for unauthorized activity for years to come.

546. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing sensitive and confidential personal, health, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

547. Further, as a result of Defendants' conduct, Plaintiffs and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at a substantial and present risk of harm.

VI. CLASS ALLEGATIONS

548. Pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), Plaintiffs bring this Action on behalf of themselves and on behalf of all other persons similarly situated. Plaintiffs propose the following Class and Subclass definitions, subject to amendment as appropriate:

> All individuals residing in the United States whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "Class");
>
> All individuals residing in the United States who entrusted their PII to Lakeview Loan Servicing, LLC and whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC n 2021 (the "Lakeview Subclass");

All individuals residing in the United States who entrusted their PII to Pingora Loan Servicing, LLC and whose PII was accessed or exfiltrated during the Data Breach announced by Pingora Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "Pingora Subclass");

All individuals residing in California whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "California Subclass");

All individuals residing in Florida whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "Florida Subclass");

All individuals residing in Georgia whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "Georgia Subclass");

All individuals residing in Illinois whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "Illinois Subclass");

All individuals residing in Indiana whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "Indiana Subclass");

All individuals residing in Maryland whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "Maryland Subclass");

All individuals residing in Missouri whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "Missouri Subclass");

All individuals residing in New York whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "New York Subclass");

All individuals residing in Ohio whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "Ohio Subclass");

All individuals residing in Pennsylvania whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "Pennsylvania Subclass");

> All individuals residing in Tennessee whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "Tennessee Subclass"); and
>
> All individuals residing in Texas whose PII was accessed or exfiltrated during the Data Breach announced by Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021 (the "Texas Subclass")

549. The Subclasses are collectively referred to herein as the "State Subclasses."

550. Excluded from the Class and the State Subclasses are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, members, affiliates, officers and directors, and any entity in which a Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff.

551. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class and Subclasses before the Court determines whether certification is appropriate.

552. Numerosity. Consistent with Fed. R. Civ. P. 23(a)(1), the Class Members are so numerous that their joinder is impracticable. Defendants' public statements indicate that the number of Class Members exceeds two and a half million. The number and identities of Class Members can be ascertained through Defendants' records.

553. Commonality. Consistent with Fed. R. Civ. P. 23(a)(2) and (b)(3), questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These questions include but are not limited to:

a. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

b. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class Members;

c. Whether Defendants had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

d. Whether Defendants had a duty not to use the PII of Plaintiffs and Class Members for non-business purposes;

e. Whether and when Defendants learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants failed to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices adequate to protect the information compromised in the Data Breach, considering its nature and scope;

i. Whether Defendants have adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Pingora violated state statutes as alleged herein;

k. Whether Lakeview violated state statutes as alleged herein;

l. Whether Bayview violated state statutes as alleged herein;

m. Whether Defendants engaged in unfair, unlawful, or deceptive practices, including by failing to safeguard the PII of Plaintiffs and Class Members;

n. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendants' wrongful conduct;

o. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

p. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

554. Typicality. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach due to Defendants' misfeasance, and their claims arise under the same legal doctrines.

555. Policies Generally Applicable to the Class. As provided under Fed. R. Civ. P. 23(b)(2), Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct in relation to the Class and making final injunctive and corresponding declaratory relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs challenge these policies by reference to Defendants' conduct with respect to the Class as a whole.

556. Adequacy of Representation. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. No Plaintiff has a disabling conflict of interest with any other Member of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class, and the infringement of rights and the damages they have suffered are typical of other Class Members. Plaintiffs also have retained counsel experienced in complex class action litigation, and they intend to prosecute this action vigorously.

557. Superiority and Manageability. Consistent with Fed. R. Civ. P. 23(b)(3), class treatment is superior to all other available methods for the fair and efficient adjudication of this

controversy. Among other things, it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Moreover, class action treatment will permit the adjudication of relatively modest claims by Class Members who could not individually afford to litigate a complex claim against large corporations such as Defendants. Prosecuting the claims pleaded herein as a class action will eliminate the possibility of repetitive litigation. There will be no material difficulty in the management of this action as a class action.

558. Particular issues, such as questions related to Defendants' liability, are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the resolution of such common issues would materially advance the resolution of this matter and the parties' interests therein.

559. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(1), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. Prosecution of separate actions by Class Members also would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class Against All Defendants)

560. Plaintiffs re-allege and incorporate paragraphs 1-559 as if fully set forth herein.

561. Plaintiffs bring this claim on behalf of themselves and the Class.

562. As a condition of receiving their mortgages or related services from Defendants or their partners or affiliates, Plaintiffs and the Class were obligated to provide and entrust them with certain PII, including their name, birthdate, address, loan number, Social Security number, and other information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

563. Plaintiffs and the Class entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

564. By undertaking the duty to maintain and secure this data, sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their systems and networks—and Plaintiffs, Class and Subclass members' PII held within it—to prevent disclosure of the information, and to safeguard the information from cyber theft.

565. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

566. Defendants knew or reasonably should have known that their failure to exercise due care in the collecting, storing, and using of consumers' PII involved an unreasonable risk of harm to Plaintiffs and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

567. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that Plaintiffs' and Class Members' information in their

possession was adequately secured and protected.

568. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former customers' or rejected loan applicants PII that they were no longer required to retain pursuant to regulations.

569. Defendants had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and the Class's PII, and to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Class.

570. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between each Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII, a mandatory step in receiving services from Defendants. While this special relationship exists independent from any contract, it is recognized by Defendants' Privacy Policies, as well as applicable laws and regulations. Specifically, Defendants actively solicited and gathered PII as part of their businesses and were solely responsible for and in the position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs, Class and Subclass members from a resulting data breach.

571. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs and the Class, to maintain adequate data security.

572. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

573. Defendants also had a common law duty to prevent foreseeable harm to others. Plaintiffs and the Class were the foreseeable and probable victims of Defendants' inadequate

security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendants' systems. It was foreseeable that Plaintiffs and Class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

574. Defendants' conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendants' wrongful conduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decision not to comply with industry standards for the safekeeping of Plaintiffs' and the Class's PII, including basic encryption techniques available to Defendants.

575. Plaintiffs and the Class had and have no ability to protect their PII that was in, and remains in, Defendants' possession.

576. Defendants were in a position to effectively protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

577. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendants' possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

578. Defendants have admitted that the PII of Plaintiffs and the Class was wrongfully accessed by unauthorized third persons as a result of the Data Breach.

579. Defendants, through their actions and inaction, unlawfully breached their duties to

Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Class when the PII was within Defendants' possession or control.

580. Defendants improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

581. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect their current and former customers' PII in the face of increased risk of theft.

582. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of their current and former customers' PII.

583. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove consumers' PII they were no longer required to retain pursuant to regulations.

584. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

585. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

586. There is a close causal connection between (a) Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Class and (b) the harm or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and the Class's PII was accessed and exfiltrated as the direct and proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

587. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of businesses, such as Defendants, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendants' duty in this regard.

588. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiffs and the Class.

589. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

590. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

591. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

592. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and

future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the current and former customers' PII in their continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class Members.

593. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

594. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

595. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs are now at an increased risk of identity theft or fraud.

596. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Lakeview Class Against Lakeview)

597. Plaintiffs re-allege and incorporate paragraphs 1-28, 31-34, 37-42, 45-50, 53-54, 57-64, 67-74, 77-82, 85-89, 96-189, 203-229, 242-278, 291-330, 341-363, 376-411, 424-466, 479-514, 526-559 as if fully set forth herein.

598. Plaintiffs bring this claim on behalf of themselves and the Lakeview Class.

599. Lakeview acquired and maintained the PII of Plaintiffs and the Lakeview Class, including names, birthdates, addresses, loan numbers, Social Security numbers, and information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

600. At the time Lakeview acquired the PII of Plaintiffs and the Lakeview Class, there was a meeting of the minds and a mutual understanding that Lakeview would safeguard the PII and not take unjustified risks when storing the PII.

601. Plaintiffs and the Lakeview Class would not have entrusted their PII to Lakeview had they known that Lakeview would make the PII internet-accessible, not encrypt sensitive data elements such as Social Security numbers, and not delete the PII that Lakeview no longer had a reasonable need to maintain.

602. Prior to the Data Breach, Lakeview published a Privacy Policy, agreeing to protect and keep private financial information of Plaintiffs and the Lakeview Class.

603. Lakeview further promised to comply with industry standards and to ensure that Plaintiffs' and Lakeview Class Members' PII would remain protected.

604. Implicit in the agreements between Plaintiffs and Lakeview Class Members and Lakeview to provide PII, was the latter's obligation to: (a) use such PII for business purposes only,

(b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Lakeview Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Lakeview Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

605. In collecting and maintaining the PII of Plaintiffs and the Lakeview Class and publishing their privacy policies, Lakeview entered into contracts with Plaintiffs and the Lakeview Class requiring Lakeview to protect and keep secure the PII of Plaintiffs and the Lakeview Class.

606. Plaintiffs and the Lakeview Class fully performed their obligations under the contracts with Lakeview.

607. Lakeview breached the contracts it made with Plaintiffs and the Lakeview Class by failing to protect and keep private financial information of Plaintiffs and the Lakeview Class, including failing to (i) encrypt or tokenize the sensitive PII of Plaintiffs and the Lakeview Class, (ii) delete such PII that Lakeview no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the internet where such accessibility was not justified, and (iv) otherwise review and improve the security of the network system that contained such PII.

608. As a direct and proximate result of Lakeview's above-described breach of implied contract, Plaintiffs and the Lakeview Class have suffered (and will continue to suffer): ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements,

and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

609. As a direct and proximate result of Lakeview's breach of contract, Plaintiffs are at an increased risk of identity theft or fraud.

610. As a direct and proximate result of Lakeview's breach of contract, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Pingora Class Against Pingora)

611. Plaintiffs re-allege and incorporate paragraphs 1-22, 29-30, 35-36, 43-44, 51-52, 55-56, 65-66, 75-76, 83-84, 90-92, 96-144, 190-202, 230-241, 279-290, 331-340, 364-375, 412-423, 467-478, 515-525, and 538-559 as if fully set forth herein. as if fully set forth herein.

612. Plaintiffs bring this claim on behalf of themselves and the Pingora Class.

613. Pingora acquired and maintained the PII of Plaintiffs and the Pingora Class, including names, birthdates, addresses, loan numbers, Social Security numbers, and information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

614. At the time Pingora acquired the PII of Plaintiffs and the Pingora Class, there was a meeting of the minds and a mutual understanding that Pingora would safeguard the PII and not take unjustified risks when storing the PII.

615. Plaintiffs and the Pingora Class would not have entrusted their PII to Pingora had they known that Pingora would make the PII internet-accessible, not encrypt sensitive data

elements such as Social Security numbers, and not delete the PII that Pingora no longer had a reasonable need to maintain.

616. Pingora further promised to comply with industry standards and to ensure that Plaintiffs' and Pingora Class Members' PII would remain protected.

617. Implicit in the agreements between Plaintiffs and Pingora Class Members and Pingora to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Pingora Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Pingora Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

618. In collecting and maintaining the PII of Plaintiffs and the Pingora Class and publishing their privacy policies, Pingora entered into contracts with Plaintiffs and the Pingora Class requiring Pingora to protect and keep secure the PII of Plaintiffs and the Pingora Class.

619. Plaintiffs and the Pingora Class fully performed their obligations under the contracts with Pingora.

620. Pingora breached the contracts it made with Plaintiffs and the Pingora Class by failing to protect and keep private financial information of Plaintiffs and the Pingora Class, including failing to (i) encrypt or tokenize the sensitive PII of Plaintiffs and the Pingora Class, (ii) delete such PII that Pingora no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the internet where such accessibility was not justified, and (iv) otherwise review and improve the security of the network system that contained such PII.

621. As a direct and proximate result of Pingora's above-described breach of implied contract, Plaintiffs and the Pingora Class have suffered (and will continue to suffer): ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

622. As a direct and proximate result of Pingora's breach of contract, Plaintiffs are at an increased risk of identity theft or fraud.

623. As a direct and proximate result of Pingora's breach of contract, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Lakeview Class Against Lakeview)

624. Plaintiffs re-allege and incorporate paragraphs 1-28, 31-34, 37-42, 45-50, 53-54, 57-64, 67-74, 77-82, 85-89, 96-189, 203-229, 242-278, 291-330, 341-363, 376-411, 424-466, 479-514, 526-559 as if fully set forth herein.as if fully set forth herein.

625. Plaintiffs bring this claim on behalf of themselves and the Lakeview Class.

626. A relationship existed between Plaintiffs and the Lakeview Class and Lakeview in which Plaintiffs and the Lakeview Class put their trust in Lakeview to protect the private information of Plaintiffs and the Lakeview Class and Lakeview accepted that trust.

627. Lakeview breached the fiduciary duty that they owed to Plaintiffs and the Lakeview Class by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiffs and the Lakeview Class.

628. Lakeview's breach of fiduciary duty was a legal cause of damage to Plaintiffs and the Lakeview Class.

629. But for Lakeview's breach of fiduciary duty, the damage to Plaintiffs and the Lakeview Class would not have occurred.

630. Lakeview's breach of fiduciary duty contributed substantially to producing the damage to Plaintiffs and the Lakeview Class.

631. As a direct and proximate result of Lakeview's breach of fiduciary duty, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Pingora Class Against Pingora)

632. Plaintiffs re-allege and incorporate paragraphs 1-22, 29-30, 35-36, 43-44, 51-52, 55-56, 65-66, 75-76, 83-84, 90-92, 96-144, 190-202, 230-241, 279-290, 331-340, 364-375, 412-423, 467-478, 515-525, and 538-559 as if fully set forth herein.

633. Plaintiffs bring this claim on behalf of themselves and the Pingora Class.

634. A relationship existed between Plaintiffs and the Pingora Class and Pingora in which Plaintiffs and the Pingora Class put their trust in Pingora to protect the private information of Plaintiffs and the Pingora Class and Lakeview accepted that trust.

635. Pingora breached the fiduciary duty that they owed to Plaintiffs and the Pingora Class by failing to act with the utmost good faith, fairness, and honesty, failing to act with the

highest and finest loyalty, and failing to protect the private information of Plaintiffs and the Pingora Class.

636. Pingora's breach of fiduciary duty was a legal cause of damage to Plaintiffs and the Pingora Class.

637. But for Pingora's breach of fiduciary duty, the damage to Plaintiffs and the Pingora Class would not have occurred.

638. Pingora's breach of fiduciary duty contributed substantially to producing the damage to Plaintiffs and the Pingora Class.

639. As a direct and proximate result of Pingora's breach of fiduciary duty, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

COUNT VI
VIOLATION OF CALIFORNIA'S CUSTOMER RECORDS ACT,
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of Plaintiffs On Behalf of Plaintiffs Derek Crenshaw, Robert Keach, and Jay Saporta and the California Subclass Against All Defendants and the California Subclass Against All Defendants)

640. Plaintiffs Derek Crenshaw, Robert Keach, and Jay Saporta ("Plaintiffs," for purposes of this Count) and the California Subclass re-allege and incorporate paragraphs 1-22, 29-30, 83-144, 190-202, 515-559 as if fully set forth herein.

641. This Count is brought on behalf of Plaintiffs and the California Subclass against all Defendants.

642. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the

information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

643. Defendants are businesses that maintain PII about Plaintiffs and California Subclass members within the meaning of Cal. Civ. Code § 1798.81.5. Such PII includes, but is not limited to, the first and last names and social security numbers of Plaintiffs and the California Subclass members, along with loan numbers and other information that would permit access to Plaintiffs and the California Subclass Members' financial accounts. *See* Cal. Civ. Code § 1798.81.5(d)(1)(A)(iii).

644. Businesses that maintain computerized data that includes PII are required to "notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b). Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

645. Defendants are businesses that maintain computerized data that includes PII as defined by Cal. Civ. Code § 1798.80.

646. Plaintiffs' and California Subclass Members' PII includes PII as covered by Cal. Civ. Code § 1798.82.

647. Because Defendants reasonably believed that Plaintiffs and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Defendants had an obligation to disclose the Data Breach immediately following their discovery to the owners or licensees of the PII (*i.e.*, Plaintiffs and the California Subclass Members) as mandated by Cal. Civ. Code § 1798.82.

648. By failing to disclose the Data Breach immediately following their discovery, Defendants violated Cal. Civ. Code § 1798.82.

649. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass Members suffered damages, as described above and as will be proven at trial.

650. Plaintiffs and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT VII
VIOLATIONS OF CALIFORNIA'S CONSUMER PRIVACY ACT,
Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")
(On Behalf of Plaintiff Derek Crenshaw, Robert Keach, and Jay Saporta and the California Subclass Against All Defendants)

651. Plaintiffs Derek Crenshaw, Robert Keach, and Jay Saporta ("Plaintiffs," for purposes of this Count) and the California Subclass re-allege and incorporate paragraphs 1-22, 29-30, 83-144, 190-202, 515-559 as if fully set forth herein.

652. This Count is brought on behalf of Plaintiffs and the California Subclass against all Defendants.

653. Defendants violated section 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent Plaintiffs' and the California Subclass' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

654. The PII of Plaintiffs and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendants' violations of their duty under the CCPA.

655. Plaintiffs and the California Subclass lost money or property, including but not limited to the loss of legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as a direct and proximate result of Defendants' acts described above.

656. Defendants knew, or should have known, that their network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII, such as properly encrypting the PII so in the event of a data breach an unauthorized third party cannot read the PII. As a result of the failure to implement reasonable security procedures and practices, the PII of Plaintiffs and members of the California Subclass was exposed.

657. Defendants are organized for the profit or financial benefit of their owners and collect PII as defined in Cal. Civ. Code § 1798.140.

658. Pursuant to § 1798.150(b) of the CCPA, Plaintiffs Robert Keach, and Jay Saporta gave written notice to Defendants Pingora and Bayview of their specific violations of section 1798.150(a) by certified mail dated April 14, 2022.[39]

659. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Derek Crenshaw gave written notice to Defendant Lakeview of its specific violations of § 1798.150(a) by certified mail dated May 4, 2022.[40]

[39] Ex. 6 (Keach et al. CCPA Notice).
[40] Ex. 7 (Crenshaw CCPA Notice).

660. Defendant Bayview did not respond. Defendant Pingora timely responded on April 29, 2021, and Defendant Lakeview timely responded on May 16, 2022,[41] but Defendants failed to "actually cure" the violations by, among other things, not retrieving and securing the lost data, not encrypting Plaintiffs' and the California Subclass's PII and/or PHI that remains on their systems, and by not deleting data they no longer have a reasonable need to maintain in an Internet accessible environment.

661. As a result, Plaintiffs and California Subclass members seek relief under § 1798.150(a) including, but not limited to, statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater; injunctive or declaratory relief; any other relief the Court deems proper; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

COUNT VIII
VIOLATION OF THE UNLAWFUL AND UNFAIR PRONG OF CALIFORNIA'S UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL")
(On Behalf of Plaintiffs Derek Crenshaw, Robert Keach, and Jay Saporta and the California Subclass Against All Defendants)

662. Plaintiffs Derek Crenshaw, Robert Keach, and Jay Saporta ("Plaintiffs," for purposes of this Count) and the California Subclass, re-allege and incorporate paragraphs 1-22, 29-30, 83-144, 190-202, 515-559 as if fully set forth herein.

663. This Count is brought on behalf of Plaintiffs and the California Subclass against all Defendants.

664. Defendants engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and the

[41] Ex. 8 (CCPA Responses).

California Subclass's PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and the California Subclass's PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and the California Subclass. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiffs and the California Subclass outweighed their utility, if any.

665. Defendants engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and the California Subclass's PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and the California Subclass. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiffs and the California Subclass outweighed their utility, if any.

666. As a direct and proximate result of Defendants' acts of unfair practices, Plaintiffs and the California Subclass were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Plaintiffs' and the California Subclass's legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

667. Defendants have also violated the UCL, Cal. Bus. & Prof. Code § 17200, *et seq*., by engaging in unlawful business acts and practices that constitute acts of "unfair competition" as defined in § 17200 of the UCL with respect to the services provided to the California Subclass.

668. Defendants engaged in unlawful acts and practices with respect to their services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and the California Subclass's PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and the California Subclass's PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to implement and maintain reasonable security procedures and practices to safeguard the PII of Plaintiffs and the California Subclass. Defendants also violated the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*. and Article 1, § 1 of the California Constitution.

669. In addition, Defendants engaged in unlawful acts and practices by failing to disclose the Data Breach to the Plaintiffs and the California Subclass in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To date, Defendants still have not provided such information to Plaintiffs and the California Subclass.

670. As a direct and proximate result of Defendants' unlawful practices and acts, Plaintiffs and the California Subclass were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of the California Subclass's legally protected interest in the confidentiality and privacy of their PII, and additional losses as described above.

671. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiffs' and the California Subclass's PII and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and the California Subclass.

672. Plaintiffs and the California Subclass seek relief under the UCL including, but not limited to, restitution to Plaintiffs and the California Subclass of money or property that the Defendants may have acquired by means of their unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

COUNT IX
VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT,
815 Ill. Comp. Stat. § 505/1, *et seq.* ("CFA")
(On Behalf of Plaintiff Beth Berg and the Illinois Subclass Against Defendants Bayview and Lakeview)

673. Plaintiff Beth Berg ("Plaintiff," for purposes of this Count) and the Illinois Subclass re-allege and incorporate paragraphs 1-22, 37-38, 87-89, 93-144, 242-253, 538-559 as if fully set forth herein.

674. Plaintiffs bring this claim on behalf of themselves and the Illinois Subclass. This Count is Brought against Defendants Bayview and Lakeview.

675. Plaintiff and the Illinois Subclass are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Illinois Subclass, and Defendants are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c). This Count is brought against Defendants Bayview and Lakeview.

676. Defendants are engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendants engage in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

677. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (1) failing to maintain adequate data security to keep Plaintiff and the Illinois Subclass's sensitive PII from being stolen by cybercriminals and

failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting material facts to Plaintiff and the Illinois Subclass regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff and the Illinois Subclass; (3) failing to disclose or omitting material facts to Plaintiff and the Illinois Subclass about Defendants' failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff and the Illinois Subclass; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and the Illinois Subclass's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

678. These actions also constitute deceptive and unfair acts or practices because Defendants knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Illinois Subclass and defeat their reasonable expectations about the security of their PII.

679. Moreover, Defendants represented that they would maintain the data they collected in a secure manner and endeavor to keep it safe from unauthorized access and exfiltration.

680. Defendants intended that Plaintiff and the Illinois Subclass rely on their deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendants' offering of goods and services.

681. Defendants' wrongful practices were and are injurious to the public because those practices were part of Defendants' generalized course of conduct that applied to the Illinois

Subclass. Plaintiff and the Illinois Subclass have been adversely affected by Defendants' conduct and the public was and is at risk as a result thereof.

682. Defendants also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Illinois Subclass of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

683. As a result of Defendants' wrongful conduct, Plaintiff and the Illinois Subclass were injured in that they never would have provided their PII to Defendants, or purchased Defendants' services, had they known or been told that Defendants failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

684. As a direct and proximate result of Defendants' violations of the CFA, Plaintiff and the Illinois Subclass have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendants that Plaintiff and the Illinois Subclass would not have made had they known of Defendants' inadequate data security; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

685. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Illinois Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the CFA.

COUNT X
VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT,
Fla. Stat. § 501.201, *et seq.* ("FDUTPA")
(On Behalf of Plaintiffs and the Class or, Alternatively, Plaintiffs Wojciechowski, Scott, and Franke and the Florida Subclass Against All Defendants)

686. Plaintiffs ("Plaintiffs," for purposes of this Count) and the Class or, alternatively, the Florida Subclass re-allege and incorporate paragraphs 1-559 as if fully set forth herein.

687. Plaintiffs bring this claim on behalf of themselves and the Class or, alternatively, the Florida Subclass. This Count is brought against all Defendants.

688. This cause of action is brought pursuant the FDUTPA, which, pursuant to Fla. Stat. § 501.202, requires such claims be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

689. Defendants' offer, provision, and sale of services at issue in this case are "consumer transaction[s]" within the scope of the FDUTPA. *See* Fla. Stat. §§ 501.201-501.213.

690. Plaintiffs and the Class Members, as "individual[s]," are "consumer[s]" as defined by the FDUTPA. *See* Fla. Stat. § 501.203(7).

691. Defendants serviced loans obtained by Plaintiffs and the Class Members.

692. Defendants offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. § 501.203.

693. Plaintiffs and the Class Members paid for or otherwise availed themselves and received services from Defendants, primarily for personal, family, or household purposes.

694. Defendants engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of loan services to or for Plaintiffs and Class Members.

695. Defendants' acts, practices, and omissions were done in the course of Defendants' businesses of offering, providing, and servicing loans throughout Florida and the United States.

696. The unfair, unconscionable, and unlawful acts and practices of Defendants alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Florida, within the scope of the FDUTPA.

697. Defendants Lakeview and Bayview, headquartered and operating in and out of Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. failure to implement and maintain reasonable and adequate computer systems and data security practices to safeguard PII;

b. omitting, suppressing, and concealing the material fact that their computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to protect the privacy and confidentiality of Plaintiffs' and Class Members' PII;

d. continued acceptance and storage of PII after Defendants knew or should have known of the security vulnerabilities that were exploited in the Data Breach;

e. continued acceptance and storage of PII after Defendants knew or should have known of the Data Breach and before it allegedly remediated the Data Breach.

698. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including by not limited to the FTC Act, 15 U.S.C. § 41, *et seq*., and the FDUTPA, Fla. Stat. § 501.171(2).

699. Defendants knew or should have known that their computer system and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and that the risk of a data breach or theft was high.

700. Plaintiffs have standing to pursue this claim because as a direct and proximate result of Defendants' violations of the FDUTPA, Plaintiffs and Class Members have been "aggrieved" by a violation of the FDUTPA and bring this action to obtain a declaratory judgment that Defendants' acts or practices violate the FDUTPA. *See* Fla. Stat. § 501.211(a).

701. Plaintiffs also have standing to pursue this claim because, as a direct result of Defendants' knowing violation of the FDUTPA, Plaintiffs are at a substantial present and imminent risk of identity theft. Defendants still possesses Plaintiffs' and the Class Members' PII, and some Plaintiffs' PII has been both accessed and misused by unauthorized third parties, which is evidence of a substantial and imminent risk of future identity theft for all Plaintiffs and Class Members.

702. Plaintiffs and Class Members are entitled to injunctive relief to protect them from the substantial and imminent risk of future identity theft, including, but not limited to:

a. ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

b. ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Defendants audit, test, and train security personnel regarding any new or modified procedures;

d. ordering that Defendants segment data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

e. ordering that Defendants purge, delete, and destroy PII not necessary for their provisions of services in a reasonably secure manner;

f. ordering that Defendants conduct regular database scans and security checks;

g. ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Defendants to meaningfully educate individuals about the threats they face as a result of the loss of their financial and PII to third parties, as well as the steps victims should take to protect themselves.

703. Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs, Class Members and the public from Defendants' unfair methods of competition and unfair, unconscionable, and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

704. The above unfair, unconscionable, and unlawful practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

705. Defendants' actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

706. Plaintiffs and Class Members seek relief under the FDUTPA, Fla. Stat. §§ 501.201, *et seq*., including, but not limited to, a declaratory judgment that Defendants' actions and/or practices violate the FDUTPA.

707. Plaintiffs and Class Members are also entitled to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

COUNT XI
VIOLATIONS OF THE MARYLAND CONSUMER PROTECTION ACT,
Md. Code Com. Law Section 13-101, *et seq.* ("MCPA")
(On Behalf of Plaintiff McMahon and the Maryland Subclass
Against Defendants Bayview and Lakeview)

708. Plaintiff McMahon ("Plaintiff," for purposes of this Count) and the Maryland Subclass re-alleges and incorporates paragraphs 1-22, 77-78, 87-89, 93-95, 479-489, and 538-559 as if fully set forth herein.

709. Plaintiffs bring this Count on their own behalf and on behalf of the Maryland Subclass. This Count is brought against Defendants Bayview and Lakeview.

710. Defendants, Plaintiff, and the Maryland Subclass are "persons" within the meaning of Md. Code Com. Law § 13-101(h).

711. The MCPA provides that a person may not engage in any unfair or deceptive trade practice in the sale of any consumer good. Md. Code Com. Law § 13-303.

712. Defendants participated in misleading, false, or deceptive acts that violated the MCPA. Defendants also intentionally concealed and suppressed material facts concerning the Data Breach and their data security practices. The following actions and omissions are examples of Defendants' tortious conduct:

a. failure to implement and maintain reasonable and adequate computer systems and data security practices to safeguard PII;

b. omitting, suppressing, and concealing the material fact that their computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to protect the privacy and confidentiality of Plaintiff's and Maryland Subclass Members' PII;

d. continued acceptance and storage of PII after Defendants knew or should have known of the security vulnerabilities that were exploited in the Data Breach; and

e. continued acceptance and storage of PII after Defendants knew or should have known of the Data Breach.

713. Plaintiff and Maryland Subclass members had limited means of discerning that Defendants' representations were false and misleading until after Defendants obtained and mishandled their PII. Thus, acting reasonably, Plaintiff and Maryland Subclass members did not and could not unravel Defendants' deception.

714. Defendants' actions as set forth above occurred in the conduct of trade or commerce.

715. Plaintiff and the Maryland Subclass members seek relief under the MCPA, Md. Code Com. Law § 13-408, including, but not limited to, actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

COUNT XII
VIOLATIONS OF THE MISSOURI MERCHANDISING PRACTICES ACT, Mo. Stat. § 407.005, *et seq*. ("MMPA")
(On Behalf of Plaintiff William Blando and the Missouri Subclass Against Defendants Bayview and Lakeview)

716. Plaintiff Blando ("Plaintiff," for purposes of this Count) and the Missouri Subclass re-allege and incorporate paragraphs 1-22, 49-50, 87-89, 93-95, 316-330, and 538-559 as if fully set forth herein.

717. This Count is brought on behalf of Plaintiff and the Missouri Subclass. This Count is brought against Defendants Bayview and Lakeview.

718. The MMPA provides:

> The act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce . . . in or from the state of Missouri is declared to be an unlawful practice.

Mo. Rev. Stat. § 407.020(1).

719. Plaintiff, the Missouri Subclass members, and Defendants are "persons" as defined in Mo. Rev. Stat. § 407.010(5).

720. Defendants advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(4), (6), and (7).

721. Plaintiff and the Missouri Subclass members purchased or leased goods or services primarily for personal, family, or household purposes.

722. By reasons of the conduct alleged herein, and by failing to provide reasonable security measure for the protection of the PII of Plaintiff and the Missouri Subclass members, Defendants violated the provisions of the MPPA, Mo. Rev. Stat. § 407.020.

723. Defendants' actions as set forth above occurred in the conduct of trade or commerce.

724. Defendants engaged in unlawful, unfair, and deceptive accts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including by:

a. failing to maintain sufficient security to keep confidential and sensitive PII of Plaintiff and the Missouri Subclass members from being hacked and stolen;

b. misrepresenting or omitting material facts to Plaintiff and the Missouri Subclass, in connection with the sales of goods and providing services, by representing that Defendants would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and the Missouri Subclass member's PII from authorized disclosure, release, data breaches, and theft;

c. misrepresenting or omitting material facts to Plaintiff and the Missouri Subclass, in connection with the sale of goods and providing services, by representing that Defendants did and would comply with the requirements of various federal and state laws pertaining to the privacy and security of Plaintiff's and Missouri Subclass members' personal information;

d. failing to prevent the Data Breach and promptly notify consumers thereof, failing to maintain the privacy and security of Plaintiff and Missouri Subclass members' personal information, in violation of duties imposed by and public policies reflected in the applicable federal and state laws; and

e. engaging in deceptive, unfair, and unlawful acts or practices by failing to disclose the Data Breach to Plaintiff and Missouri Subclass members in a timely and accurate manner.

725. Due to the Data Breach, Plaintiff and the Missouri Subclass have lost property in the form of their PII and have suffered actual damages. Further, Defendants' failure to adopt reasonable practices in protecting and safeguarding the confidential and sensitive PII of their customers has resulted in Plaintiff and the Missouri Subclass spending time and money to protect against identify theft. Plaintiff and the Missouri Subclass members are now at a higher risk of identity theft crimes. This harm sufficiently outweighs any justification or motives for Defendants' practice of collecting and storing confidential and sensitive PII without the appropriate and reasonable safeguards to protect such information.

726. As a result of Defendants' practices and conduct, Plaintiff and the Missouri Subclass members have suffered injury-in-fact and have lost money or property. As a result of Defendants' failure to adopt, implement, and maintain reasonable security procedures, and the resulting Data Breach, Plaintiff and the Missouri Subclass members have incurred costs and spent time associated with monitoring and repairing issues from the loss of PII and issues of identity theft.

727. Plaintiff and the Missouri Subclass members seek relief under the MMPA, Mo. Rev. Stat. § 407.025, including, but not limited to, declaratory and injunctive relief, actual

damages, punitive damages, attorneys' fees, costs, and such other relief as the Court deems just and proper.

COUNT XIII
VIOLATIONS OF THE INDIANA DECEPTIVE CONSUMER SALES ACT, Ind. Code § 24-5-0.5-1, *et seq*. ("IDCSA")
(On Behalf of Plaintiff Savannah Farley and the Indiana Subclass Against Defendants Bayview and Lakeview)

728. Plaintiff Savannah Farley ("Plaintiff," for purposes of this Count) and the Indiana Subclass re-allege and incorporate paragraphs 1-22, 39-40, 87-89, 93-95, 254-264, and 538-559 as if fully set forth herein.

729. This Count is brought by Plaintiff on behalf of the Indiana Subclass. This Count is brought against Defendants Bayview and Lakeview.

730. Ind. Code § 24-5-0.5-3(a) prohibits suppliers from engaging in deceptive, unfair, and abusive acts or omissions in consumer transactions.

731. Defendants are each a "supplier" who engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of "consumer transactions," in violation of the IDCSA. As a regular part of their businesses, Defendants provide mortgage loans and related products to individuals residing in Indiana. Defendants accept payments from customers, like Plaintiff, online, in person or by mail. Transactions were directed towards Indiana, and on information and belief, those transactions were processed in Indiana.

732. In connection with their consumer transactions, Defendants engaged in unfair, abusive or deceptive acts, omissions or practices by, *inter alia*, engaging in the following conduct:

a. failing to maintain sufficient security to keep sensitive PII of Plaintiff and the Indiana Subclass members from being hacked and stolen;

b. misrepresenting material facts to Plaintiff and the Indiana Subclass members in connection with the sale of goods or services, by representing that they would maintain adequate data privacy and security practices and procedures to safeguard their PII from unauthorized disclosure, release, data breaches, and theft, including but not limited to promises made in their privacy policies;

c. misrepresenting material facts to Plaintiff and the Indiana Subclass members, in connection with the sale of goods and services, by representing that Defendants did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of their PII, such requirements included, but are not limited to, those imposed by laws such as the Federal Trade Commission Act (15 U.S.C. § 45) and Indiana's data breach statute (Ind. Code § 24-4.9-3.5); and

d. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and the Indiana Subclass members' PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

733. Defendants knew that their computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and the Indiana Subclass members, and that risk of a data breach or theft was highly likely. Nevertheless, they did nothing to warn them about their data insecurities, and instead affirmatively promised that they would maintain adequate security. This was a deliberate effort to mislead customers, such as Plaintiff and the Indiana Subclass members, to encourage them to use Defendants' services.

734. The above unfair and deceptive practices and acts by Defendants were done as part of a scheme, artifice, or device with intent to defraud or mislead and constitute incurable deceptive acts under the IDCSA.

735. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and the Indiana Subclass members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their financial and personal information and damages.

736. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and the Indiana Subclass members are now likely to suffer identity theft crimes, and they face a lifetime risk of identity theft crimes.

737. The IDCSA provides that "[a] person relying upon an uncured or incurable deceptive act may bring an action for the damages actually suffered as a consumer as a result of the deceptive act or five hundred dollars ($500), whichever is greater." § 24-5-0.5-4(a). Moreover, "[t]he court may increase damages for a willful deceptive act in an amount that does not exceed the greater of: (1) three (3) times the actual damages of the consumer suffering the loss; or (2) one thousand dollars ($1,000)." Id.

738. The IDCSA provides that a senior consumer, defined as "an individual who is at least sixty (60) years of age," may recover treble damages for an incurable deceptive act. Id. §§ 24-5-0.5-2(a)(9), 24-5-0.5-4(i).

739. Plaintiff and the Indiana Subclass members seek relief under Ind. Code § 24-5-0.5-4, including, but not limited to, the maximum statutory damages available under the IDCSA, restitution, penalties, injunctive relief, and/or attorneys' fees and costs.

COUNT XIV
VIOLATIONS OF THE TEXAS DECEPTIVE TRADE PRACTICES – CONSUMER PROTECTION ACT
Texas Bus. & Com. Code § 17.41, *et seq*.
(On Behalf of Plaintiffs Stone, Gonzales, and Myers and the Texas Subclass Against Defendants Bayview and Lakeview)

740. Plaintiffs Stone, Gonzales, and Myers ("Plaintiffs," for purposes of this Count) and the Texas Subclass re-allege and incorporate paragraphs 1-22, 25-28, 81-82, 87-89, 93-95, 161-189, 503-514, and 538-559 as if fully set forth herein.

741. Plaintiffs bring this claim on behalf of themselves and the Texas Subclass. This Count is brought against Defendants Bayview and Lakeview.

742. Defendants "person[s]" as defined by Tex. Bus. & Com. Code § 17.45(3).

743. Plaintiffs and the Texas Subclass members are "consumer[s]" as defined by Tex. Bus. & Com. Code § 17.45(4).

744. Defendants advertised, offered, or sold services in Texas and engaged in trade or commerce directly or indirectly affecting the people of the state of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

745. Defendants engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code §§ 17.46(b)(5), (7), and (9), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which the person does not;

b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another;

c. Advertising goods or services with intent not to sell them as advertised.

746. Defendants' false, misleading and deceptive acts and practices include:

a. Failing to protect the PII in their possession;

b. Failing to implement and maintain adequate, industry-standard computer systems and allowing unauthorized access to and exfiltration of Plaintiffs' and Texas Subclass members' PII, which was a direct and proximate cause of the Data Breach;

c. Failing to identify and remedy foreseeable security and privacy risks;

d. Failing to disclose the material fact that Defendants' computer systems and data security practices were inadequate to safeguard the PII in their possession from theft;

e. Failing to disclose in a timely and accurate manner to Plaintiffs and the Texas Subclass members the material fact of the Data Breach; and

f. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Texas Subclass members' PII;

747. Defendants intended to mislead Plaintiffs and Texas Subclass members and induce them to rely on their misrepresentations and omissions.

748. Defendants' misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy and security of Defendants' data storage systems and Defendants' ability to protect consumers' PII.

749. Plaintiffs and Texas Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions and could not have discovered Defendants' data systems were actually inadequate.

750. Had Defendants disclosed to Plaintiffs and Texas Subclass members that their data

systems were not secure and therefore vulnerable to attack, Plaintiffs and Texas Subclass members would not have relinquished their private information and Defendants would have been forced to adopt adequate data security practices to comply with the law and continue doing business.

751. Defendants owed a common law duty to prevent foreseeable harm to Plaintiffs and Texas Subclass members. The duty existed because Plaintiffs and Texas Subclass members provided their PII in exchange for Defendants' services, and they were the foreseeable and probable victims of any inadequate security practices of Defendants in their collection, storage, and use of PII from Plaintiffs and Texas Subclass members. It was foreseeable that Plaintiffs and Texas Subclass members would be harmed by the failure to protect their PII because malicious actors routinely attempt to steal such information for nefarious purposes.

752. Defendants violated § 17.50(a)(1) by representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which the person does not; representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and advertising goods or services with intent not to sell them as advertised. Consumers relied on these misrepresentations and omissions to consumers' own detriment.

753. Defendants alone knew about the deficiencies of their data systems. Consumers, including Plaintiffs and Texas Subclass members, lacked this knowledge because this information was known exclusively by Defendants, and consumers lack expertise in information security. Even if they did have this expertise, consumers do not have access to Defendants' data systems to ensure the security of their PII.

754. As a direct and proximate result of Defendants' violations as alleged above,

Plaintiffs and Texas Subclass members have suffered, will suffer, or are at increased risk of suffering:

g. The compromise, publication, theft and/or unauthorized use of their PII;

h. Unauthorized use and misuse of their PII;

i. The loss of the opportunity to control how their PII is used;

j. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

k. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

l. The present and imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

m. The continued risk to their PII that is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PII in Defendants' possession; and

n. Current and future costs in terms of time, effort and money that they will expend to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of their lives.

755. Plaintiffs noticed Defendants of the violations and injuries complained of herein as required by Tex. Bus. & Com. Code Ann. § 17.505 and Defendants have failed to cure those violations within the time prescribed by statute.

756. Plaintiffs and Texas Subclass members seek all monetary and non-monetary relief as the court deems just and proper.

COUNT XV
VIOLATION OF THE OHIO RESIDENTIAL MORTGAGE LOAN ACT
Ohio Rev. Code § 1322.01, *et seq*. ("RMLA")
(On behalf of Plaintiff Shannon Thomas and the Ohio Subclass
Against Defendants Bayview and Lakeview)

757. Plaintiff Shannon Thomas ("Plaintiff," for purposes of this Count) and the Ohio Subclass re-allege and incorporate paragraphs 1-22, 79-80, 87-89, 93-95, 279-290, and 538-559 as if fully set forth herein.

758. Plaintiffs bring this claim on behalf of themselves and the Ohio Subclass. This Count is brought against Defendants Bayview and Lakeview.

759. Defendants are each a registrant, licensee, and a person required to be registered or licensed under the RMLA. As such, Defendants cannot "[e]ngage in conduct that constitutes improper, fraudulent, dishonest dealings." Ohio Rev. Code § 1322.40(C).

760. In addition, a registrant, licensee, or person required to be registered or licensed under the RMLA is required to comply with all duties imposed by other statutes or common law, act with reasonable skill, care, and diligence and act in good faith and with fair dealing in any transaction, practice, or course of business in connection with the brokering or originating of any residential mortgage loan. Ohio Rev. Code § 1322.45(A).

761. Defendants' failures to implement and maintain reasonable security measures with respect to Plaintiff's and the Ohio Subclass members' PII violated the RMLA.

762. As a result of Defendants' conduct, Plaintiff and the Ohio Subclass members have suffered and will continue to suffer foreseeable harm. Plaintiff and Ohio Subclass members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses

and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and present and an increased risk of future harm.

763. Plaintiff and Ohio Subclass members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

764. Plaintiff and Ohio Subclass members seek damages, punitive damages, reasonable attorneys' fees and costs pursuant to Ohio Rev. Code § 1322.45(D), and any other relief the court deems just and proper.

COUNT XVI
VIOLATIONS OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW,
73 Pa. Stat. § 201-1, *et seq.*
(On behalf of Plaintiff David Kraus and the Pennsylvania Subclass Against Defendants Bayview and Pingora)

765. Plaintiff David Kraus ("Plaintiff," for purposes of this Count) and the Pennsylvania Subclass re-allege and incorporate paragraphs 1-22, 75-76, 90-92, 93-95, 467-478, and 538-559 as if fully set forth herein.

766. Plaintiff brings this claim on behalf of himself and the Pennsylvania Subclass. This Count is brought against Defendants Bayview and Pingora.

767. Plaintiff, Pennsylvania Subclass members, and Defendants are "persons" as defined by 73 Pa. Stat. § 201-2(2).

768. Plaintiff and Pennsylvania Subclass members purchased goods and services in "trade" and "commerce" as defined by 73 Pa. Stat. § 201-2(3).

769. Plaintiff and Pennsylvania Subclass members purchased goods and services primarily for personal, family, and/or household purposes under 73 Pa. Stat. § 201-9.2.

770. Defendants engaged in "unfair methods of competition" or "unfair or deceptive acts or practices" as defined by 73 Pa. Stat. § 201-2(4) by, among other things, engaging in the following conduct:

a. Representing that their goods and services had characteristics, uses, benefits, and qualities that they did not have – namely that their goods, services, and business practices were accompanied by adequate data security (73 Pa. Stat. § 201-2(4)(v));

b. Representing that their goods and services were of a particular standard or quality when they were of another standard or quality (73 Pa. Stat. § 201-2(4)(vii));

c. Advertising their goods and services with intent not to sell them as advertised (73 Pa. Stat. § 201-2(4)(ix)); and

d. "Engaging in any other . . . deceptive conduct which creates a likelihood of confusion or of misunderstanding" (73 Pa. Stat. § 201-2(4)(xxi)).

771. These unfair methods of competition and unfair or deceptive acts or practices are declared unlawful by 73 Pa. Stat. § 201-3.

772. Defendants' unfair or deceptive acts and practices include but are not limited to:

a. failing to implement and maintain reasonable data security measures to protect Personal Information;

b. failing to identify foreseeable data security risks and remediate the identified risks;

c. failing to comply with common law duties, industry standards, and FTC guidance regarding data security; and

d. omitting and concealing the material fact that it did not have reasonable measures in place to safeguard such Personal Information.

773. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security practices and ability to protect customers' Personal Information.

774. Defendants intended to mislead consumers and induce them to rely on their misrepresentations and omissions, and Plaintiff and Pennsylvania Subclass members did rely on Defendants' misrepresentations and omissions relating to their data privacy and security.

775. Plaintiff and Pennsylvania Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered with reasonable diligence.

776. Had Defendants disclosed to consumers that their data security systems were not secure and, thus, were vulnerable to attack, Plaintiff and Pennsylvania Subclass members would not have given their Personal Information to Defendants.

777. Defendants acted intentionally, knowingly, and maliciously in violating 73 Pa. Stat. § 201-1, *et seq.*, and recklessly disregarded consumers' rights.

778. As a direct and proximate result of Defendants violation of violating 73 Pa. Stat. § 201-1, *et seq.*, Plaintiff and Pennsylvania Subclass members have suffered and will continue to suffer damages, injury, ascertainable losses of money or property, and monetary and non-monetary damages as alleged herein.

779. Plaintiff and Pennsylvania Subclass members seek all remedies available under 73 Pa. Stat. § 201-1, *et seq.*, including, but not limited to, the damages expressly permitted under 73 Pa. Stat. § 201-9.2: actual damages or statutory damages of $100, whichever is greater; treble damages defined as three time the actual damages; reasonable attorneys' fees and litigation costs; and any other such additional relief the Court deems necessary or proper.

780. Plaintiff and Pennsylvania Subclass members also seek injunctive relief as set forth herein.

COUNT XVII
VIOLATIONS OF THE TENNESSEE IDENTITY THEFT DETERRENCE ACT OF 1999
Tenn. Code. Ann § 47-18-2101, *et seq.*
(On behalf of Plaintiff April Burnett and the Tennessee Subclass Against Defendants Bayview and Lakeview)

781. Plaintiff April Burnett ("Plaintiff," for purposes of this Count) and the Tennessee Subclass re-allege and incorporate paragraphs 1-22, 61-62, 87-89, 93-95, 388-399, and 538-559 as if fully set forth herein.

782. Plaintiff brings this count on behalf of the Tennessee Subclass. This Count is brought against Defendants Bayview and Lakeview.

783. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

784. Plaintiff and Tennessee Subclass members' Personal Information that was compromised in the Data Breach includes Personal Information as covered under Tenn. Code Ann. § 47-18-2107(a)(3)(A).

785. Defendants are required to accurately notify Plaintiff and Tennessee Subclass members if they become aware of a breach of their data security systems that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Tennessee Subclass members'

Personal Information in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

786. Because Defendants discovered a breach of their security systems in which unencrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person, Defendants have an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

787. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Tenn. Code Ann. § 47-18-2107(b).

788. As a direct and proximate result of Defendants' violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass members suffered damages, as described above.

789. Plaintiff and Tennessee Subclass members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages and injunctive relief.

COUNT XVIII
VIOLATIONS OF THE TENNESSEE CONSUMER PROTECTION ACT OF 1977, Tenn. Code. Ann § 47-18-101, *et seq.*
(On behalf of Plaintiff April Burnett and the Tennessee Subclass Against Defendants Bayview and Lakeview)

790. Plaintiff April Burnett ("Plaintiff," for purposes of this Count) and the Tennessee Subclass re-allege and incorporate paragraphs 1-22, 61-62, 87-89, 93-95, 388-399, and 538-559 as if fully set forth herein.

791. Plaintiff brings this count on behalf of the Tennessee Subclass. This Count is brought against Defendants Bayview and Lakeview.

792. Tenn. Code Ann. § 47-18-109(a)(1) provides that "[a]ny person who suffers an ascertainable loss of money or property, real, personal, or mixed, or any other article, commodity,

or thing of value wherever situated, as a result of the use or employment by another person of an unfair or deceptive act or practice described in § 47-18-104(b) and declared to be unlawful by this part, may bring an action individually to recover actual damage."

793. Tenn. Code Ann. § 47-18-109(a)(3) further provides that "[i]f the court finds that the use or employment of the unfair or deceptive act or practice was willful or knowing violation of this part, the court may award three (3) times the actual damages sustained and may provide such other relief as it considers necessary and proper…."

794. Defendants' mortgage services constitute "trade or commerce."

795. Defendants' conduct violates the Tennessee Consumer Protection Act because Defendants engaged in the deceptive acts and practices described above, which included a failure to protect Plaintiff's and the Tennessee Subclass's Personal Information in spite of assurances to the contrary.

796. Defendants omitted material facts concerning the steps they took (or failed to undertake) to protect Plaintiff and Tennessee Subclass members' Personal Information, which were deceptive, false and misleading given the conduct described herein. Such conduct is inherently and materially deceptive and misleading in a material respect, which Defendants knew, or by the exercise of reasonable care, should have known, to be untrue, deceptive or misleading. Such conduct is unfair, deceptive, untrue, or misleading in that Defendants: (a) represented that their services have approval, characteristics, uses or benefits that they do not have; and (b) represented that services are of a particular standard, quality or grade.

797. Defendants' materially misleading statements and deceptive acts and practices alleged herein were directed at the public at large.

798. Defendants' actions impact the public interest because Plaintiff and the Tennessee Subclass have been injured in exactly the same way as thousands of others as a result of and pursuant to Defendants' generalized course of deception as described throughout this Complaint.

799. Defendants' acts and practices described above were likely to mislead a reasonable consumer acting reasonably under the circumstances.

800. Defendants' misrepresentations, misleading statements and omissions were materially misleading to Plaintiff and members of the Tennessee Subclass.

801. Defendants' violation of Tenn. Code Ann. § 47-18-104 was willful and knowing. As described above, at all relevant times, Defendants, among other things, knew that their policies and procedures for the protection of Plaintiff's and the Tennessee Subclass' PII were inadequate to protect that PII. Nonetheless, Defendants continued to solicit and process PII in the United States in order to increase their own profits.

802. Had Plaintiff and the members of the Tennessee Subclass known of Defendants' misrepresentations, misleading statements and omissions about their use of PII, they would not have purchased Defendants' services and given Defendants or Defendants' partners their PII.

803. As a direct and proximate result of Defendants' conduct in violation of Tenn. Code Ann. § 47-18-104, Plaintiff and the members of the Tennessee Subclass have been injured in amounts to be proven at trial.

804. As a result, pursuant to Tenn. Code Ann. §§ 47-18-104 and 47-18-109, Plaintiff and the Tennessee Subclass are entitled to damages in an amount to be determined at trial. Burnett also properly asks that such damages be trebled based on Defendants' knowledge and/or intention with respect to their breach.

805. Plaintiff also seeks injunctive relief, including a robust, state of the art notice program for the wide dissemination of a factually accurate statement on the actual state of Defendants' PII storage and the implementation of a corrective advertising campaign by Defendants.

806. Additionally, pursuant to Tenn. Code Ann. § 47-18-109, Plaintiff and the Tennessee Subclass make claims for attorneys' fees and costs.

COUNT XIX
VIOLATIONS OF THE GEORGIA SECURITY BREACH NOTIFICATION ACT, O.C.G.A. § 10-1-912, *et seq.*
(On behalf of Plaintiff Deborah Hamilton and the Georgia Subclass Against Defendants Bayview and Lakeview)

807. Plaintiff Deborah Hamilton ("Plaintiff," for purposes of this Count) re-alleges and incorporates paragraphs 1-22, 33-34, 87-89, 93-95, 218-229, and 538-559 as if fully set forth herein.

808. Plaintiff brings this count on behalf of the Georgia Subclass. This Count is brought against Defendants Bayview and Lakeview.

809. Defendants are businesses that own or license computerized data that includes PII as defined by O.C.G.A. § 10-1-912(a).

810. Plaintiff and Georgia Subclass members' Personal Information that was compromised in the Data Breach includes PII covered under O.C.G.A. § 10-1-912(a).

811. Defendants are required to accurately notify Plaintiff and Georgia Subclass members if they become aware of a breach of their data security systems that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Subclass members' PII in the most expedient time possible and without unreasonable delay under O.C.G.A. § 10-1-912(a).

812. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated O.C.G.A. § 10-1-912(a).

813. As a direct and proximate result of Defendants' violations of O.C.G.A. § 10-1-912(a), Plaintiff and Georgia Subclass members suffered damages, as described above.

814. Plaintiff and Georgia Subclass members seek relief under O.C.G.A. § 10-1-912, including actual damages and injunctive relief.

COUNT XX
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW,
N.Y. Gen. Bus. Law § 349, *et seq.*
(On behalf of Plaintiff Hardik Sevak and the NewYork Subclass
Against Defendants Bayview and Lakeview)

815. Plaintiff Hardik Sevak ("Plaintiff," for purposes of this Count) re-alleges and incorporates paragraphs 1-22, 47-48, 87-89, 93-95, 303-315, and 538-559 as if fully set forth herein.

816. Plaintiff brings this count on behalf of the New York Subclass. This Count is brought against Defendants Bayview and Lakeview.

817. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Yor Subclass Members' PII, which was a proximate and direct cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' PII, including by implementing and maintaining reasonable security measures;

d. Failing to timely and adequately notify the Plaintiff and Class Members of the Data Breach;

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' PII; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, and N.Y. Gen. Bus. Law § 899-aa.

818. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

819. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff's and New York Subclass members' rights.

820. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

821. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large.

822. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

823. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

COUNT XXI
VIOLATIONS OF INFORMATION SECURITY BREACH AND NOTIFICATION ACT, N.Y. Gen. Bus. Law § 899-aa
(On behalf of Plaintiff Hardik Sevak and the New York Subclass Against Defendants Bayview and Lakeview)

824. Plaintiff Hardik Sevak ("Plaintiff," for purposes of this Count) re-alleges and incorporates paragraphs incorporates paragraphs 1-22, 47-48, 87-89, 93-95, 303-315, and 538-559 as if fully set forth herein.as if fully set forth herein.

825. Plaintiff brings this count on behalf of the New York Subclass. This Count is brought against Defendants Bayview and Lakeview.

826. Defendants are each a business that owns or licenses computerized data that includes Personal Information as defined by N.Y. Gen. Bus. Law § 899-aa(1)(a). Defendants also maintain computerized data that includes PII which Defendants do not own. Accordingly, they are subject to N.Y. Gen. Bus. Law §§ 899- aa(2) and (3).

827. Plaintiff's and New York Subclass members' private information (e.g. Social Security numbers) includes PII covered by N.Y. Gen. Bus. Law § 899-aa(1)(b).

828. Defendants are required to give immediate notice of a breach of security of a data system to owners of PII which Defendants do not own, including Plaintiff and New York Subclass members, pursuant to N.Y. Gen. Bus. Law § 899-aa(3).

829. Defendants are required to accurately notify Plaintiff and New York Subclass members if it discovers a security breach or receives notice of a security breach which may have compromised PII which Defendants own or license, in the most expedient time possible and without unreasonable delay under N.Y. Gen. Bus. Law § 899-aa(2).

830. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

831. As a direct and proximate result of Defendants violations of N.Y. Gen. Bus. Law §§ 899-aa(2) and (3), Plaintiff and New York Subclass members suffered damages, as described above.

832. Plaintiff and New York Subclass members seek relief under N.Y. Gen. Bus. Law § 899-aa(6)(b), including actual damages and injunctive relief.

COUNT XXII
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class Against All Defendants)

833. Plaintiffs re-allege and incorporate paragraphs 1-559 as if fully set forth herein.

834. Plaintiffs bring this count on behalf of themselves and the Class. This count is brought against all Defendants.

835. The Declaratory Judgment Act, 28 U.S.C. § 2201, *et. seq*., authorizes this Court to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

836. Defendants owe duties of care to Plaintiffs and Class Members which require them to adequately secure their PII.

837. Defendants still possesses Plaintiffs' and Class members' PII.

838. Defendants do not specify in their Data Breach notification letters what steps they have taken to prevent a similar breach from occurring again.

839. Plaintiffs and Class Members are at risk of harm due to the exposure of their PII and Defendants' failures to address the security failings that lead to such exposure.

840. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and the Class Members' PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and the Class from further data breaches that compromise their PII.

841. Plaintiffs and the Class, therefore, seek a declaration that (1) each of Defendants' existing security measures do not comply with their obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect consumers' Personal Information, and (2) to comply with their duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

d. Segmenting user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiffs and Class Members for their respective lifetimes; and

h. Meaningfully educating Plaintiffs and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

842. The Court should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with the law and industry standards to protect Plaintiffs' and Class Members' PII.

843. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendants' systems or networks. The risk of another breach is real, immediate, and substantial.

844. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. If another data breach occurs, Plaintiffs and the Class will likely be subjected to fraud, identity theft, and other harms described herein. But, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is minimal given they have pre-existing legal obligations to employ these measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against Defendants and that the Court grant the following:

A. An Order certifying the Class and the State Subclasses, as defined herein, and appointing Plaintiffs and their counsel to represent the Class and State Subclasses;

B. Equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and the Class Members;

C. Injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;

iv. requiring Defendants to delete, destroy, and purge the PII of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

vi. prohibiting Defendants from maintaining Plaintiffs' and Class Members' personally identifying information on a cloud-based database;

vii. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

x. requiring Defendants to segment data by, among other things, creating firewalls

and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other areas of Defendants' systems;

xi. requiring Defendants to conduct regular database scanning and securing checks;

xii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personally identifying information, as well as protecting the personally identifying information of Plaintiffs and Class Members;

xiii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personally identifying information;

xv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and

updated;

xvi. requiring Defendants to adequately educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and, for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to Class Counsel, and to report any material deficiencies or noncompliance with the Court's final judgment;

D. For an award of damages, including actual, statutory, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of reasonable attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: August 1, 2022

Respectfully submitted,

/s/ Julie Braman Kane
Julie Braman Kane
Florida Bar No. 980277
COLSON HICKS EIDSON
255 Alhambra Circle – Penthouse
Coral Gables, Florida 33134
Telephone: (305) 476-7400
Facsimile: (305) 476-7444
julie@colson.com
Liaison Counsel

JOHN A. YANCHUNIS
RYAN D. MAXEY
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com
Chair, Executive Committee

M. ANDERSON BERRY (*pro hac vice*)
GREGORY HAROUTUNIAN (*pro hac vice* forthcoming)
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

RACHELE R. BYRD (*pro hac vice*)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599
byrd@whafh.com

ADAM E. POLK (*pro hac vice*)
JORDAN ELIAS (*pro hac vice*)
SIMON GRILLE (*pro hac vice*)
KIMBERLY MACEY (*pro hac vice*)
GIRARD SHARP LLP
601 California St, Ste 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
apolk@girardsharp.com
jelias@girardsharp.com
sgrille@girardsharp.com
kmacey@girardsharp.com

JOSEPH M. LYON (*pro hac vice* forthcoming)
THE LYON FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Telephone: (513) 381-2333
jlyon@thelyonfirm.com

GARY M. KLINGER (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

DAVID K. LIETZ (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
Email: dlietz@milberg.com

STUART ANDREW DAVIDSON
BRADLEY BEALL
NICOLE BRITO
Robbins Geller Rudman & Dowd LLP
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
561-750-3000
Fax: 750-3364
Email: sdavidson@rgrdlaw.com
bbeall@rgrdlaw.com
nbrito@rgrdlaw.com

TERRY R. COATES (*pro hac vice*)
DYLAN J. GOULD (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: 513/651-3700
513/665-0219 (fax)
tcoates@msdlegal.com
dgould@msdlegal.com

LORI G. FELDMAN *(pro hac vice)*
GEORGE GESTEN
MCDONALD, PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Phone: (917) 983-9321
Fax: (888) 421-4173
Email: LFeldman@4-Justice.com
E-Service: eService@4-Justice.com

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

The undersigned certifies that, on August 1, 2022, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF. I also certify the foregoing document is being served today on all counsel of record in this case via transmission of Notice of Electronic Filing generated by CM/ECF.

/s/Julie Braman Kane
JULIE BRAMAN KANE